

# An algebraic framework for end-to-end physical-layer network coding

Elisa Gorla and Alberto Ravagnani\*

Institut de Mathématiques  
Université de Neuchâtel  
Emile-Argand 11, CH-2000 Neuchâtel, Switzerland

## Abstract

We propose an algebraic setup for end-to-end physical-layer network coding based on submodule transmission. We introduce a distance function between modules, describe how it relates to information loss and errors, and show how to compute it. Then we propose a definition of submodule error-correcting code, and investigate bounds and constructions for such codes.

## Introduction and motivation

In the framework of physical-layer network coding (PNC) multiple terminals attempt to exchange messages through intermediate relays. The relays collect data from the terminals, and try to decode a function of the transmitted messages. Such function is then broadcasted to the terminals, which combine it with their side information to recover the other messages.

In [11] the authors proposed a novel approach to PNC based on nested lattices, known as “compute-and-forward”. Under this approach, the structure of a fixed underlying lattice is exploited by the relays to decode the function of the messages, which is then forwarded to the terminals. As observed in [5], this communication scheme induces an end-to-end network coding channel with channel equation

$$Y = AX + Z. \quad (1)$$

Here  $X$  is the transmitted matrix, whose rows are elements from a given ambient space  $\Omega$ ,  $A$  is a transfer matrix, and  $Z$  is an error matrix. In practice,  $A$  and  $Z$  are random matrices drawn according to certain distributions, that depend on the application at hand.

A general algebraic framework to study and construct nested-lattice-based PNC schemes was recently proposed in [5] and further developed in [4]. Following this algebraic description, which is compatible with any underlying lattice, the message space  $\Omega$  has the structure of a module over a principal ideal ring

$$\Omega = T/(d_1) \times T/(d_2) \times \dots \times T/(d_n),$$

where  $T \subseteq \mathbb{C}$  is a principal ideal domain (PID),  $d_1, d_2, \dots, d_n \in T$  are nonzero, non-invertible elements, and  $d_n | d_{n-1} | \dots | d_1$ . Let  $R = T/(d_1)$ , then  $R$  is a principal ideal ring (PIR). The ambient space  $\Omega$  is isomorphic to an  $R$ -submodule of  $R^n$ :

$$\Omega \cong R \times (d_1/d_2) \times \dots \times (d_1/d_n) \subseteq R^n. \quad (2)$$

---

\*E-mail addresses: [elisa.gorla@unine.ch](mailto:elisa.gorla@unine.ch), [ravagnani@ece.utoronto.ca](mailto:ravagnani@ece.utoronto.ca). The authors were partially supported by the Swiss National Science Foundation through grant no. 200021\_150207.

In particular, the elements of  $\Omega$  can be represented via vectors of length  $n$  with entries in  $R$ . Both  $R$  and  $\Omega$  are usually finite.

**Examples 1.** We include a list of rings  $R$  and ambient spaces  $\Omega$  that have been proposed in the context of physical-layer network coding, producing efficient communication schemes.

- $R = \Omega = \mathbb{Z}_2[i]$ , proposed and studied in [15], [12] and [4, Example 1] for BPSK modulation.
- $R = \Omega = \mathbb{Z}_m[i]$ , with  $m$  a positive integer, proposed and studied in [15] and [4, Example 2], and known as “ $m^2$ -QAM PNC scheme”.
- $R = \mathbb{Z}_p[i]$ ,  $\Omega = R^n$ , where  $p$  is a prime number, proposed in [11].
- $R = \mathbb{Z}_{p^s}[i]$ ,  $\Omega = \underbrace{R \times \dots \times R}_{n_1} \times \underbrace{(p) \times \dots \times (p)}_{n_2} \times \dots \times \underbrace{(p^{s-1}) \times \dots \times (p^{s-1})}_{n_s}$ , where  $p$  is a prime power and  $s \geq 1$  is an integer, proposed in [4, Section VII.A].
- $R = \mathbb{Z}[\omega]/(\beta)$ , where  $\mathbb{Z}[\omega]$  are the Eisenstein integers and  $\beta \in \mathbb{Z}[\omega]$  is a suitable element,  $\Omega = R^n$ , proposed and studied in [13].

As observed in [5], channel equation (1) suggests to define the message to be transmitted as the module generated over  $R$  by the rows of the matrix  $X$ , which we denote by  $\text{row}(X)$ . A receiver attempts to recover the original transmitted module from the matrix  $Y$ .

Two important special cases of equation (1) correspond to the **noise-free multiplicative matrix channel** (MMC), with equation  $Y = AX$ , and the **multiplication-free additive matrix channel** (AMC), with equation  $Y = X + Z$ . These two channel equations are studied in [5] in the case where the base ring  $R$  is a finite chain ring.

The key tool in handling the MMC in [5] is the reduced row-echelon form of a matrix  $X$ , which is a canonical invariant of the row-module of  $X$  denoted by  $\text{RREF}(X)$ . In practice, a transmitter emits a matrix  $X$  in reduced row-echelon form, and a receiver attempts to recover it by computing  $\text{RREF}(Y) = \text{RREF}(AX)$ . Decoding is successful when  $A$  is left-invertible. In the same paper, the authors propose a coding/decoding scheme based on error-trapping for the AMC and the general case of a channel with equation (1).

In this paper, in analogy with the approach from [8] for random linear network coding, we propose a new algebraic framework for module transmission based on the notion of length of a module. We define a submodule code as a collection of submodules of the ambient space  $\Omega$ , and propose a notion of distance between submodules based on length, which we call submodule distance. Then we show that the submodule distance captures both information loss and errors in module transmissions. The row-echelon form for modules over a PIR proposed by Buchmann and Neis in [2] allows us to represent messages in a canonical way. Using the same row-echelon form, we reduce the computation of the distance between submodules to the computation of the length of ideals in the base ring. We also prove that, in some cases, the error-trapping decoding scheme from [5] is a minimum-distance decoding with respect to the submodule distance.

We derive two bounds on the cardinality of a submodule code of given minimum distance and whose codewords have fixed length. For certain classes of rings, we are able to state our bounds explicitly in terms of the ring and code’s invariants. We also construct submodule codes with maximum error-correction capability. For  $R$  a finite chain ring or  $R = \mathbb{Z}_p[i]$ , we show that the codes that we construct have asymptotically optimal cardinality for their parameters. This also shows that our bounds are sharp for certain choices of rings and code parameters. We also give some general code constructions, based on the tensor and on the cartesian product. Our constructions can be applied to various choices of rings and code parameters.

Finally, we study codes over products of rings. This is relevant, since a finite PIR  $R$  is isomorphic to a product of finite fields and finite chain rings. We show that if  $R \cong R_1 \times \dots \times R_m$ , then a product of codes on the  $R_i$ 's yields a code on  $R$ , whose parameters are determined and whose decoding can be reduced to decoding on each of the  $R_i$ 's. However, not every code over a finite PIR is a product of codes over fields and finite chain rings. We give a construction of a code over  $R$  which is not a product and show that decoding cannot be reduced to decoding on each of the  $R_i$ 's. This shows in particular how the study of codes over a finite PIR cannot be reduced to the study of codes over finite fields and finite chain rings.

The structure of the paper is as follows: In Section 1 we recall some definitions and results about PIR's, modules, length, row-echelon forms of matrices over PIR's. In Section 2 we define submodule codes and submodule distance, and relate it to information loss and errors in module transmissions. We also show how to efficiently compute the submodule distance. In Section 3 we prove that, in some cases, the error-trapping decoding from [5] can be viewed as a minimum-distance decoding in our framework. Section 4 is devoted to bounds on the cardinality of submodule codes, and Section 5 to submodule codes constructions and to codes over products of rings.

## 1 Algebraic preliminaries

Throughout the paper  $R$  denotes a finite PIR and  $(r)$  denotes the ideal generated by  $r \in R$ . Recall that elements  $a, b \in R$  generate the same ideal if and only if they are **associate**, i.e., there exists an invertible element  $\varepsilon \in R$  with  $a = \varepsilon b$  (see e.g. [1]). An element  $g \in R$  is a **greatest common divisor (gcd)** of  $a_1, \dots, a_s \in R$  if and only if  $(a_1) + (a_2) + \dots + (a_s) = (g)$ . We write  $g = \gcd(a_1, \dots, a_s)$ . The gcd is unique up to associates.

**Finite chain rings** are a special case of PIR's. A ring  $R$  is a finite chain ring if it is finite and its ideals form a chain with respect to inclusion. It is well-known that finite chain rings are principal and local (see e.g. [10], page 339). Moreover, if  $\pi$  is a generator of the maximal ideal of  $R$ , then the ideals of  $R$  are

$$0 \subsetneq (\pi^{e-1}) \subsetneq (\pi^{e-2}) \subsetneq \dots \subsetneq (\pi) \subsetneq R, \quad (3)$$

where  $e$  is the smallest positive integer with  $\pi^e = 0$ . The integer  $e$  does not depend on the choice of the generator  $\pi$  of the maximal ideal. The finite field  $R/(\pi)$  is called the **residue field** of  $R$ . Clearly,  $R/(\pi) \cong \mathbb{F}_q$  for some prime power  $q$ .

For any PIR  $R$ , define the **annihilator** of  $a \in R$  as

$$\text{ann}(a) = \{r \in R \mid ar = 0\}.$$

The annihilator is an ideal of  $R$ , and we refer to a generator of  $\text{ann}(a)$  again as the **annihilator** of  $a$ . If  $R$  is a finite chain ring with ideal chain as in (3), then every  $a \in R$  is of the form  $a = u\pi^\alpha$  for some invertible  $u$  and some  $0 \leq \alpha \leq e$ . Then  $\text{ann}(a) = (\pi^{e-\alpha})$ . Since every finite PIR  $R$  is isomorphic to a product of finite fields and finite chain rings, then annihilators are easy to compute. In the sequel, we will take computation of annihilators for granted. Moreover, inclusion of annihilators can be easily tested by checking divisibility.

**Proposition 2.** Let  $R$  be a finite PIR,  $a, b \in R$ . Then  $\text{ann}(a) \subseteq \text{ann}(b)$  if and only if  $a \mid b$ .

*Proof.* By the Zariski-Samuel Theorem, any finite PIR is isomorphic to a product of finite fields and finite chain rings. Hence it suffices to prove the statement for  $R$  a finite chain ring. If  $b = ac$  for some  $c \in R$ , then  $tb = tac = 0$  for every  $t \in \text{ann}(a)$ . Hence  $\text{ann}(a) \subseteq \text{ann}(b)$ . Conversely, if

$\text{ann}(a) \subseteq \text{ann}(b)$  and  $R$  is a finite chain ring with ideal chain as in (3), then  $a = u\pi^\alpha$  and  $b = v\pi^\beta$  for some  $u, v$  invertible,  $0 \leq \alpha, \beta \leq e$ . Since  $(\pi^{e-\alpha}) = \text{ann}(a) \subseteq \text{ann}(b) = (\pi^{e-\beta})$ , then  $e - \alpha \geq e - \beta$ , so  $\alpha \leq \beta$  and  $a \mid b$ .  $\square$

## 1.1 Modules and length

We fix an  $R$ -module  $\Omega \subseteq R^n$  as in (2) and let  $\mathcal{M}(\Omega)$  denote the set of  $R$ -submodules of  $\Omega$ . Given  $M, N \in \mathcal{M}(\Omega)$ , denote by  $M + N$  the smallest submodule of  $\Omega$  which contains both  $M$  and  $N$ . We write  $M \oplus N$  when  $N \cap M = 0$ . Since  $R$  is finite,  $\Omega$  and its submodules are finite. In particular all modules that we consider are finitely generated.

**Definition 3.** Let  $M$  be an  $R$ -module. If

$$M = \{r_1 m_1 + \dots + r_t m_t \mid r_1, \dots, r_t \in R\}$$

for some  $m_1, \dots, m_t \in M$ , then we say that  $M$  is **generated** by  $m_1, \dots, m_t$  and  $m_1, \dots, m_t$  are a **system of generators** for  $M$ . We write  $M = \langle m_1, \dots, m_t \rangle_R$  or  $M = \langle m_1, \dots, m_t \rangle$  when there is no ambiguity. A module is **finitely generated** if it has a finite system of generators.

**Definition 4.** Let  $M$  be an  $R$ -module. A chain of distinct submodules of  $M$  of the form

$$0 \subsetneq M_1 \subsetneq M_2 \subsetneq \dots \subsetneq M_\lambda = M$$

has **length**  $\lambda$ . The **length** of  $M$  is

$$\lambda_R(M) = \max\{\lambda \mid M \text{ has a chain of } R\text{-submodules of length } \lambda\}.$$

A **composition series** for  $M$  is a maximal chain of distinct  $R$ -submodules of  $M$ .

When the ring is clear from context, we will omit the subscript  $R$ .

**Remark 5.** Any ring  $R$  is an  $R$ -module, and its  $R$ -submodules coincide with its ideals. Therefore, the length of a ring  $R$  is

$$\lambda(R) = \max\{\lambda \mid R \text{ has a chain of ideals of length } \lambda\}.$$

For any  $a \in R$  we denote by  $\lambda(a)$  the length of the ideal generated by  $a$ .

Since all modules that we consider are finite, they have finite length. The following properties are well-known (see e.g. [9, Section V§2]).

**Lemma 6.** Let  $R$  be a ring, let  $M, N, \Omega$  be  $R$ -modules of finite length. Then:

- 1)  $\lambda(M) = 0$  if and only if  $M = 0$ .
- 2) If  $N \subseteq M$ , then  $\lambda(N) \leq \lambda(M)$  and  $\lambda(M/N) = \lambda(M) - \lambda(N)$ . In particular,  $\lambda(M) = \lambda(N)$  if and only if  $M = N$ .
- 3) If  $M, N \subseteq \Omega$ , then  $\lambda(M + N) = \lambda(M) + \lambda(N) - \lambda(M \cap N)$ .
- 4)  $\lambda(M \times N) = \lambda(M) + \lambda(N)$ .

The concept of length for an  $R$ -module generalizes the concept of dimension for a vector space.

**Example 7** (fields). Every field  $\mathbb{F}$  is a ring of length one, since it has no proper nonzero ideals. An  $\mathbb{F}$ -module  $M$  is an  $\mathbb{F}$ -vector space with  $\lambda(M) = \dim_{\mathbb{F}}(M)$ .

**Example 8** (finite chain rings). Let  $R$  be a finite chain ring. Let  $\pi$  be a generator of its maximal ideal and let  $e$  be the smallest positive integer such that  $\pi^e = 0$ . Then  $\lambda(R) = e$  and  $\lambda(a) = \min\{i : a \in (\pi^{e-i})\} = \min\{i : \pi^{e-i} \mid a\}$  for all  $a \in R$ .

It can be shown that every  $R$ -module  $M$  is isomorphic to a product of ideals:

$$M \cong \underbrace{R \times \dots \times R}_{\mu_1} \times \underbrace{(\pi) \times \dots \times (\pi)}_{\mu_2 - \mu_1} \times \dots \times \underbrace{(\pi^{e-1}) \times \dots \times (\pi^{e-1})}_{\mu_e - \mu_{e-1}},$$

where  $0 \leq \mu_1 \leq \mu_2 \leq \dots \leq \mu_e$  are non-negative integers. Following [5], we say that  $M$  has **shape**  $(\mu_1, \mu_2, \dots, \mu_e) \in \mathbb{N}^e$ . It is easy to show that two  $R$ -modules are isomorphic if and only if they have the same shape. Moreover, by Lemma 6

$$\lambda(M) = \sum_{i=0}^{e-1} (\mu_{i+1} - \mu_i)(e - i),$$

where  $\mu_0 = 0$ .

## 1.2 A reduced row-echelon form for matrices over principal ideal rings

Every finitely generated module  $M \subseteq \Omega$  may be represented as the rowspace of a matrix with entries in  $R$ , whose row vectors are a system of generators of  $M$ . In order to make such a representation unique, we need a row-canonical form for matrices with entries in a PIR.

In [7] Howell proposes a definition of row-canonical matrix over the ring  $\mathbb{Z}_n$ , showing that every matrix can be put in row-canonical form by performing invertible row operations. The ideas of Howell were later extended in [2], where canonical generating systems for submodules of  $R^n$  are defined for any PIR  $R$ . In the rest of the section we recall the main results of [2], stating them in a convenient matrix formulation.

**Definition 9.** For  $i \in \{1, \dots, n\}$  we denote by  $v_i$  the  $i$ -th entry of a vector  $v \in R^n$ . The **leading position** of a vector  $v \in R^n$  is the position of its first nonzero entry:

$$\ell(v) = \begin{cases} \min\{1 \leq j \leq n \mid v_j \neq 0\} & \text{if } v \neq 0, \\ +\infty & \text{if } v = 0. \end{cases}$$

Given a matrix  $A \in R^{t \times n}$ , we denote by  $A_1, \dots, A_t$  the rows of  $A$ , and by  $\text{row}(A) = \langle A_1, \dots, A_t \rangle$  the  $R$ -module generated by the rows of  $A$ .

For a module  $M \subseteq R^n$  we set  $M^{(j)} = \{v \in M \mid v_i = 0 \text{ for } i < j\}$  for  $j \in \{1, \dots, n+1\}$ . Every  $M^{(j)}$  is an  $R$ -submodule of  $M$  and

$$0 = M^{(n+1)} \subseteq M^{(n)} \subseteq \dots \subseteq M^{(1)} = M.$$

**Definition 10.** Let  $A \in R^{t \times k}$  be a matrix, and let  $M = \text{row}(A)$ . We say that  $A$  is in **row-echelon form** if the following hold:

- 1) for all  $i \in \{1, \dots, t-1\}$  we have  $\ell(A_{i+1}) > \ell(A_i)$ ,
- 2) for all  $j \in \{1, \dots, n+1\}$  we have  $M^{(j)} = \langle A_i \mid \ell(A_i) \geq j \rangle$ .

The nonzero entries of  $A$  of the form  $A_{i,\ell(A_i)}$  are the **pivots** of  $A$ .

Fix canonical generators and representatives for the ideals and the residue classes of  $R$ . We say that  $A$  is in **reduced row-echelon form** if it is in row-echelon form and the following hold:

- 3) every pivot  $A_{ij}$  of  $A$  is the canonical generator of the ideal  $(A_{ij})$ ,
- 4) if  $A_{ij}$  is a pivot of  $A$ , then every entry  $A_{sj}$  with  $s < i$  is the canonical representative of the residue class  $A_{sj} + (A_{ij})$ .

**Definition 11.** Two matrices  $A, B \in R^{t \times n}$  are **row-equivalent** if there exists an invertible matrix  $U \in R^{t \times t}$  such that  $A = UB$ .

It is easy to show that  $A$  and  $B$  are row-equivalent if and only if  $\text{row}(A) = \text{row}(B)$ . We now prove that every matrix is row-equivalent to a matrix in row-echelon form, and to a unique matrix in reduced row-echelon form. The next lemma is well-known and appears in several references. We include a proof, since we could not find a complete one in the literature.

**Lemma 12.** For any  $a, b \in R \setminus \{0\}$  there exist  $x, y, z, t \in R$  such that

$$\begin{bmatrix} x & y \\ z & t \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} g \\ 0 \end{bmatrix}, \quad xt - yz = 1, \quad (g) = (a) + (b).$$

*Proof.* By [14, Theorem 33, pg. 245], every principal ideal ring is isomorphic to a direct product of quotients of PID's. Therefore it suffices to prove the result for  $R = D/(\pi)$ , where  $D$  is a PID and  $\pi \in D$ .

If  $\pi = 0$  then  $R = D$  is a PID. Let  $g = \gcd(a, b)$  and write  $g = ka + hb$  for some  $k, h \in R$ . Dividing by  $g$  we obtain  $1 = k(a/g) + h(b/g)$ . Let  $x = k, y = h, z = -b/g, t = a/g$ .

Now assume  $\pi \neq 0$ . Recall that every PID  $D$  is a unique factorization domain. Consider the projection map  $\bar{\cdot} : D \rightarrow R$  and choose elements  $\alpha, \beta \in D$  with  $\bar{\alpha} = a$  and  $\bar{\beta} = b$ . Let  $\eta = \gcd(\alpha, \beta, \pi)$  and  $P = \{p \in D \mid p \text{ is irreducible and divides both } \alpha/\eta \text{ and } \pi/\eta\}$ . For all  $p \in P$  we set  $e_p = \max\{i \mid p^i \text{ divides } \pi/\eta\}$ . Define

$$\gamma = \begin{cases} (\pi/\eta) / \prod_{p \in P} p^{e_p} & \text{if } P \neq \emptyset, \\ (\pi/\eta) & \text{if } P = \emptyset. \end{cases}$$

We claim that  $\alpha/\eta + \gamma(\beta/\eta)$  and  $\pi/\eta$  are coprime. By contradiction, let  $p \in D$  be irreducible,  $p \mid \gcd(\pi/\eta, \alpha/\eta + \gamma(\beta/\eta))$ . If  $p \nmid \gamma$ , then  $p \mid \prod_{p \in P} p^{e_p}$ , so  $p \mid (\alpha/\eta)$ . Since  $\gcd(\alpha/\eta, \beta/\eta, \pi/\eta) = 1$  and  $p \mid (\alpha/\eta), (\pi/\eta)$ , then  $p \nmid \alpha/\eta + \gamma(\beta/\eta)$ , a contradiction. If  $p \mid \gamma$ , then  $p \nmid \prod_{p \in P} p^{e_p}$ , so  $p \nmid (\alpha/\eta)$ . However  $p \mid (\alpha/\eta + \gamma(\beta/\eta))$ , a contradiction. We conclude that  $\alpha/\eta + \gamma(\beta/\eta)$  and  $\pi/\eta$  are coprime, hence there exist  $\lambda, \mu \in D$  such that  $\lambda(\alpha/\eta + \gamma(\beta/\eta)) + \mu(\pi/\eta) = 1$ , i.e.  $\lambda(\alpha + \gamma\beta) + \mu\pi = \eta$ . Hence

$$(\eta) \subseteq (\alpha + \gamma\beta, \pi) \subseteq (\alpha, \beta, \pi) = (\eta).$$

Therefore  $(\alpha + \gamma\beta) + (\pi) = (\alpha) + (\beta) + (\pi)$ , so  $a + cb = \gcd(a, b)$  in  $R = D/(\pi)$ , where  $c = \bar{\gamma}$ . Write  $b = h(a + cb)$ , for some  $h \in R$ . Let  $x = 1, y = c, z = -h, t = -ch + 1$ .  $\square$

**Remark 13.** The element  $\gamma \in D$  in the proof of Lemma 12 can be computed (up to associates) via the following algorithm.

```

 $\gamma := \pi/\eta$ 
 $g := \gcd(\gamma, \alpha/\eta)$ 
while  $g \neq 1$  do
```

$\gamma \leftarrow \gamma/g$   
 $g \leftarrow \gcd(\gamma, \alpha/\eta)$   
**end while**

**Theorem 14** ([2], Algorithm 3.2 and Theorem 3.3). Given a matrix  $A \in R^{t \times k}$ , we can compute a row-equivalent matrix in row-echelon form in  $\mathcal{O}(tk^2)$  operations in  $R$ .

We describe Algorithm 3.2 from [2], adapting it to our matrix notation.

- 1) If  $A$  is the zero matrix, then it is already in row-echelon form. Otherwise, up to permuting the rows of  $A$ , we may assume without loss of generality that  $+\infty > \ell(A_1) \geq \ell(A_2) \geq \dots \geq \ell(A_t)$ .
- 2) If  $j = \ell(A_1) > \ell(A_2)$  then the first step is concluded. Otherwise, let  $g = \gcd(A_{1j}, A_{2j}, \dots, A_{tj})$ . Applying Lemma 12 iteratively one finds a row-equivalent matrix  $A' \in R^{t \times n}$  with  $A'_{1j} = g$  and  $\ell(A'_i) > j$  for  $i > 1$ .
- 3) Let  $x \in R$  be the annihilator of  $g$ . We append  $x \cdot A_1$  to the matrix  $A'$ , obtaining a matrix  $A''$ . Notice that  $\text{row}(A'') = \text{row}(A)$ . Moreover, if  $v \in \text{row}(A'')$  and  $v_s = 0$  for  $1 \leq s \leq j$ , then  $v \in \langle A''_2, \dots, A''_{t+1} \rangle$ .

One repeats the three steps above on the matrix obtained from  $A''$  by deleting the first row, until there are no more rows left. The algorithm produces a matrix in row-echelon form, which is row-equivalent to  $A$ .

**Example 15.** Consider the matrix

$$A = \begin{bmatrix} 2 & 1 & 3 \\ 4 & 1 & 2 \end{bmatrix}$$

over  $R = \mathbb{Z}_6$ . Applying the algorithm that we just described, one computes:

$$\begin{bmatrix} 2 & 1 & 3 \\ 4 & 1 & 2 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 2 & 1 & 3 \\ 0 & 5 & 2 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 2 & 1 & 3 \\ 0 & 3 & 3 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 2 & 1 & 3 \\ 0 & 5 & 2 \\ 0 & 0 & 3 \end{bmatrix}.$$

Notice that the number of rows increased from two to three.

Fix generators and representatives for the ideals and residue classes of  $R$ . Every matrix  $A$  with entries in  $R$  is row-equivalent to a unique matrix in reduced row-echelon form, with respect to the given choice of generators and representatives.

**Theorem 16** ([2], Algorithm 3.4 and Theorem 3.5). Let  $A \in R^{t \times n}$  be a matrix. Then  $A$  is row-equivalent to a unique matrix in reduced row-echelon form, which we denote by  $\text{RREF}(A)$ . The reduced row-echelon form of  $A$  can be computed from a row-echelon form of  $A$  in  $\mathcal{O}(n^3)$  operations in  $R$ .

In fact, using the algorithm from Theorem 14,  $A$  can be put in row-echelon form. After multiplying it by a diagonal matrix with invertible elements on the diagonal, the matrix satisfies property 3) of Definition 10. Finally, by subtracting suitable multiples of each row from the rows above, one ensures that property 4) of Definition 10 holds. The last operation corresponds to multiplying on the left by an upper triangular matrix with ones on the diagonal.

The next result characterizes matrices in row-echelon form over a finite PIR. A proof can be obtained using Proposition 2.

**Proposition 17.** Let  $A \in R^{t \times n}$  be a matrix with no zero rows.  $A$  is in row-echelon form if and only if the following hold:

1.  $\ell(A_{i+1}) > \ell(A_i)$  for all  $i \in \{1, \dots, t-1\}$ ,
2.  $A_{t\ell(A_t)} \mid A_{tj}$  for all  $\ell(A_t) \leq j \leq n$ ,
3.  $\text{ann}(A_{i\ell(A_i)}) \cdot A_i \in \langle A_{i+1}, \dots, A_t \rangle$  for all  $i \in \{1, \dots, t-1\}$ .

Proposition 17 and Algorithm 4.1 of [2] lead to the following algorithm to test whether a matrix is in row-echelon form.

**Input:** a matrix  $A \in R^{t \times n}$  with  $\ell(A_{i+1}) > \ell(A_i)$  for all  $i \in \{1, \dots, t-1\}$

**Output:** “YES” if  $A$  is in row-echelon form, and “NO” otherwise

**for**  $i = 1$  **to**  $t$  **do**

$j_i := \ell(A_i)$

**end for**

**for**  $j = j_t$  **to**  $n$  **do**

**if**  $A_{tj_t} \nmid A_{tj}$  **then**

**return** NO

**quit**

**end if**

**end for**

**for**  $i = t-1$  **downto**  $1$  **do**

use Algorithm 4.1 of [2] to test if  $\text{ann}(A_{ij_i}) \cdot A_i \in \langle A_{i+1}, \dots, A_t \rangle$

**if**  $\text{ann}(A_{ij_i}) \cdot A_i \notin \langle A_{i+1}, \dots, A_t \rangle$  **then**

**return** NO

**quit**

**end if**

**end for**

**return** YES

**quit**

**Proposition 18.** The previous algorithm terminates correctly.

*Proof.* Algorithm 4.1 of [2] tests whether a given vector belongs to the module generated by the rows of a matrix in row-echelon form. Therefore, we first need to show that the last **for** cycle of the algorithm is well-defined, i.e., that if the algorithm enters the **for** cycle for some  $i$ , then the matrix whose rows are  $A_{i+1}, \dots, A_t$  is in row-echelon form.

We proceed by backward induction on  $i \in \{t-1, \dots, 1\}$ . Assume that the algorithm enters the cycle for  $i = t-1$ . Then by the structure of the algorithm and Proposition 17, the matrix whose row is  $A_t$  is in row-echelon form, as claimed. Now assume  $i < t-1$ . Since the algorithm enters the **for** cycle for  $i$ , it entered the **for** cycle also for  $i+1$ . By induction hypothesis, the matrix whose rows are  $A_{i+2}, \dots, A_t$  is in row-echelon form. Since the algorithm enters the **for** cycle for  $i$ , we have  $\text{ann}(A_{i+1}) \cdot A_{i+1} \in \langle A_{i+2}, \dots, A_t \rangle$ . Therefore by Proposition 17 the matrix whose rows are  $A_{i+1}, \dots, A_t$  is in row-echelon form.

The previous argument also shows that if the algorithm returns YES, then  $A$  is in row-echelon form. Finally, using Proposition 17 one can check that if  $A$  is in row-echelon form, then the algorithm returns YES.  $\square$



## 2 Submodule codes and submodule distance

Using the length, one can define a distance function between submodules of  $\Omega$ .

**Proposition 19.** The function  $d : \mathcal{M}(\Omega) \times \mathcal{M}(\Omega) \rightarrow \mathbb{N}$  defined by

$$d(M, N) = \lambda(M) + \lambda(N) - 2\lambda(M \cap N)$$

for all  $M, N \in \mathcal{M}(\Omega)$  is a distance function.

**Definition 20.** We call  $d$  the **submodule distance** on  $\mathcal{M}(\Omega)$ .

*Proof of Proposition 19.* Let  $M, N, P \subseteq \Omega$  be  $R$ -submodules. By Lemma 6 we have  $d(M, N) = \lambda(M + N) - \lambda(M \cap N)$ . Since  $M \cap N \subseteq M + N$  we have  $d(M, N) \geq 0$ , and equality holds if and only if  $M + N = M \cap N$ , i.e., if and only if  $M = N$ . Moreover,  $d(M, N) = d(N, M)$  by definition.

To prove the triangular inequality, observe that by definition

$$d(M, N) = d(M, P) + d(P, N) - 2(\lambda(M \cap N) + \lambda(P) - \lambda(M \cap P) - \lambda(N \cap P)).$$

Therefore it suffices to prove that  $x = \lambda(M \cap N) + \lambda(P) - \lambda(M \cap P) - \lambda(N \cap P) \geq 0$ . By Lemma 6 we have  $x = \lambda(M + P) + \lambda(N + P) - \lambda(M + N) - \lambda(P)$ . Since  $(M + P) + (N + P) \supseteq M + N$  and  $(M + P) \cap (N + P) \supseteq P$ , by Lemma 6

$$\lambda(M + P) + \lambda(N + P) - \lambda(P) \geq \lambda(M + P) + \lambda(N + P) - \lambda((M + P) \cap (N + P)) \geq \lambda(M + N),$$

hence  $x \geq 0$ .  $\square$

When  $R = \mathbb{F}$  is a field, the submodule distance on  $\mathbb{F}^n$  coincides with the **subspace distance** proposed by Kötter and Kschischang in [8] for error correction in random linear network coding.

The concepts of information loss and error from [8] can be extended to our setting as follows.

**Remark 21.** Let  $M \subseteq R^n$  be the transmitted module, and let  $N \subseteq R^n$  be the received module. The portion of information that was correctly transmitted is  $M \cap N$ . The quotient  $M/(M \cap N)$  may be regarded as the **information loss module**, i.e. the original information modulo the portion of information that was correctly transmitted. Similarly, the **error module** is the quotient  $N/(M \cap N)$ . Using Lemma 6, one can check that

$$d(M, N) = \lambda(M/(M \cap N)) + \lambda(N/(M \cap N)).$$

In other words, the distance between  $M$  and  $N$  is the sum of the lengths of the information loss module and of the error module, similarly to what was shown in [8] in the context of subspace codes.

**Definition 22.** A **submodule code** is a subset  $\mathcal{C} \subseteq \mathcal{M}(\Omega)$  with  $|\mathcal{C}| \geq 2$ . The **minimum (submodule) distance** of  $\mathcal{C}$  is

$$d(\mathcal{C}) = \min\{d(M, N) : M, N \in \mathcal{C}, M \neq N\}.$$

**Definition 23.** Let  $\mathcal{C} \subseteq \mathcal{M}(\Omega)$  be a submodule code. Let  $M \in \mathcal{C}$  be the transmitted module, and let  $N \in \mathcal{M}(R^n)$  be the received module. Define the **number of erasures** as  $\rho = \lambda(M/(M \cap N))$  and the **number of errors** as  $e = \lambda(N/(M \cap N))$ .

The next result follows from Remark 21 using a standard argument.

**Proposition 24.** Let  $\mathcal{C} \subseteq \mathcal{M}(\Omega)$  be a submodule code of minimum distance  $d$ . Then a minimum distance decoder successfully corrects  $N$  to  $M$ , provided that  $2(\rho + e) < d(\mathcal{C})$ .

## 2.1 Computing the distance function

In this subsection we show that the length of a module is the sum of the lengths of the ideals generated by the pivots of a matrix in row-echelon form, whose rows generate the module. Therefore, computing the length of an  $R$ -module can be reduced to computing lengths of ideals in  $R$ . This allows us to efficiently compute distances between submodules of  $R^n$ .

**Theorem 25.** Let  $M \subseteq R^n$  be an  $R$ -module. Let  $A \in R^{t \times n}$  be a matrix in row-echelon form with no zero rows and such that  $M = \text{row}(A)$ . For every  $j \in \{1, \dots, n+1\}$  let  $M^{(j)} = \{m \in M \mid v_i = 0 \text{ for } i < j\} \subseteq R^n$  and  $I^{(j)} = (v_j \mid v \in M^{(j)}) \subseteq R$ . Let  $A_{i\ell(A_i)}$  be the pivot of the  $i$ -th row of  $A$ . Then:

- 1)  $I^{(\ell(A_i))} = (A_{i\ell(A_i)}) \cong M^{(j)}/M^{(j+1)}$  for all  $i \in \{1, \dots, t\}$ ,
- 2)  $\lambda(M) = \sum_{i=1}^t \lambda(A_{i\ell(A_i)})$ .

*Proof.* 1) The map  $M^{(j)}/M^{(j+1)} \rightarrow I^{(j)}$  given by  $v + M^{(j+1)} \mapsto v_j$  is a well-defined  $R$ -module isomorphism. Therefore  $I^{(j)} \cong M^{(j)}/M^{(j+1)}$ . Fix any  $i \in \{1, \dots, t\}$  and let  $j = \ell(A_i)$ . Since  $A_i \in M^{(j)}$  we have  $(A_{ij}) \subseteq I^{(j)}$ . On the other hand, let  $0 \neq x \in I^{(j)}$  and let  $v \in M^{(j)}$  such that  $x = v_j$ . Since  $A$  is in row-echelon form,  $v = \sum_{k=i}^t r_k A_k$  for some  $r_i, \dots, r_t \in R$ . Therefore  $x = v_j = r_i A_{ij}$ , so  $x \in (A_{ij})$ .

- 2) Applying [9, Corollary V.2.4] to the chain of  $R$ -modules  $0 = M^{(n+1)} \subseteq \dots \subseteq M^{(1)} = M$  we obtain

$$\lambda(M) = \sum_{j=1}^n \lambda(M^{(j)}/M^{(j+1)}).$$

By Lemma 6 one has  $\lambda(M^{(j)}/M^{(j+1)}) \neq 0$  if and only if  $I^{(j)} \neq 0$ , if and only if  $j = \ell(A_i)$  for some  $i \in \{1, \dots, t\}$ . Then

$$\lambda(M^{(j)}/M^{(j+1)}) = \lambda(A_{ij}).$$

□

**Example 26.** The module  $M = \langle (2, 1, 3), (4, 1, 2) \rangle \subseteq \mathbb{Z}_6^3$  generated by the rows of the matrix of Example 15 has length  $\lambda(M) = \lambda(2) + \lambda(5) + \lambda(3) = 1 + 2 + 1 = 4$ .

**Remark 27.** Let  $M = \text{row}(A)$  be the transmitted module, and let  $N = \text{row}(B)$  be the received module. By Lemma 6 we have

$$d(M, N) = 2\lambda(M + N) - \lambda(M) - \lambda(N).$$

Therefore the distance between  $M$  and  $N$  can be computed from the row-echelon forms of  $A$ ,  $B$ , and of the matrix  $C$  obtained by appending the rows of  $B$  to  $A$ . In fact

$$M + N = \text{row}(A) + \text{row}(B) = \text{row}(C).$$

This allows us to compute the distance function without computing intersections of modules.

**Example 28.** Let  $R = \mathbb{Z}_4$ . Notice that the only nonzero, proper ideal of  $R$  is  $(2)$ . Let

$$A = \begin{bmatrix} \underline{1} & 1 & 1 & 0 \\ 0 & \underline{2} & 1 & 2 \\ 0 & 0 & \underline{2} & 0 \end{bmatrix}, \quad B = \begin{bmatrix} \underline{1} & 3 & 0 & 2 \\ 0 & 0 & \underline{1} & 0 \end{bmatrix}$$

be matrices in row-echelon form, whose underlined entries are the pivots. Let  $M = \text{row}(A)$  and  $N = \text{row}(B)$ . Then

$$\begin{aligned}\lambda(M) &= \lambda(1) + \lambda(2) + \lambda(2) = 2 + 1 + 1 = 4 \\ \lambda(N) &= \lambda(1) + \lambda(1) = 2 + 2 = 4\end{aligned}$$

Then  $M + N = \text{row}(C)$ , where

$$C = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 2 & 1 & 2 \\ 0 & 0 & 2 & 0 \\ 1 & 3 & 0 & 2 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

whose reduced row-echelon form is

$$\begin{bmatrix} \underline{1} & 1 & 0 & 0 \\ 0 & \underline{2} & 0 & 2 \\ 0 & 0 & \underline{1} & 0 \end{bmatrix}.$$

Hence  $\lambda(M + N) = \lambda(1) + \lambda(2) + \lambda(1) = 2 + 1 + 2 = 5$  and

$$d(M, N) = 2\lambda(M + N) - \lambda(M) - \lambda(N) = 10 - 8 = 2.$$

One can compute  $\lambda(M \cap N) = \lambda(M) + \lambda(N) - \lambda(M + N) = 3$ . Hence the information loss module has length  $\lambda(M/(M \cap N)) = \lambda(M) - \lambda(M \cap N) = 1$  and the error module has length  $\lambda(N/(M \cap N)) = \lambda(N) - \lambda(M \cap N) = 1$ .

### 3 Recovering known encoding and decoding schemes

In this section we compare our approach to the one proposed by Feng, Nóbrega, Kschischang, and Silva for the multiplicative-additive matrix channel (MAMC) in [4, Section IX]. We show that their encoding scheme remains valid in our setup. We also prove that, in some cases, their decoding scheme corresponds to minimum distance decoding with respect to the distance function that we propose.

In our notation, Feng, Nóbrega, Kschischang, and Silva consider the MAMC of equation  $Y = AX + Z$ , where  $R$  is a finite chain ring,  $A \in R^{N \times t}$ ,  $X \in R^{t \times n}$ ,  $Z \in R^{N \times n}$ . They assume that  $n \geq 2N$ ,  $\text{row}(A) \cong R^t$ , and  $\text{row}(Z) \cong R^v$  for some integer  $v \leq N$ . They represent matrices in **row canonical form** (see [4, Definition 1] for the definition of row canonical form) and define their codebook to be the set of **principal** matrices of given shape in row canonical form (see [4, Section V.B and Sections VII, VIII, IX]). Observe that matrices in row canonical form are not in general in reduced row-echelon form according to our Definition 10.

**Example 29.** Let  $R = \mathbb{Z}_8$ , whose ideals  $0 \subsetneq (4) \subsetneq (2) \subsetneq (1)$  have canonical generators  $0, 4, 2, 1$ . Choose  $0, 1, 2, 3$  as canonical representatives for residue classes modulo  $(4)$ ,  $0, 1$  as canonical representatives for residue classes modulo  $(2)$ , and  $0$  as canonical representative for the residue class modulo  $(1)$ . The rows of the following matrices generate the same  $R$ -module. The first matrix is in row canonical form (see [4, Example 6]), while the second is in reduced row-echelon form. The pivots are underlined.

$$\begin{bmatrix} 0 & 2 & 0 & \underline{1} \\ \underline{2} & 2 & 0 & 0 \\ 0 & 0 & \underline{2} & 0 \\ 0 & \underline{4} & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} \underline{2} & 0 & 0 & 1 \\ 0 & \underline{2} & 0 & 1 \\ 0 & 0 & \underline{2} & 0 \\ 0 & 0 & 0 & \underline{2} \end{bmatrix}.$$

The authors of [4] propose asymptotically optimal encoding and decoding schemes using principal matrices over a finite chain ring  $R$ . A transmitted module  $M$  is encoded as a principal matrix in row canonical form, whose rows generate  $M$ . In the next proposition we show that principal matrices in row canonical form are in reduced row-echelon form. Therefore, the encoding schemes of [4] remain valid in our setup.

**Proposition 30.** Let  $R$  be a finite chain ring, and let  $A \in R^{t \times n}$  be a principal matrix in row canonical form. Then  $A$  is in reduced row-echelon form with respect to the same choices of generators and representatives.

*Proof.* Let  $\pi$  be a generator of the maximal ideal of  $R$ , let  $e$  be the smallest positive integer such that  $\pi^e = 0$ . By the definition of principal row canonical form, the pivot of row  $A_i$  is  $A_{ii} = \pi^{\ell_i}$  for  $i \in \{1, \dots, t\}$ , with  $0 \leq \ell_1 \leq \dots \leq \ell_t \leq e$ . Moreover,  $A_{ij} = \pi^{a_{ij}}$  with  $a_{ij} \geq \ell_i$  for  $i < j \leq n$ , hence  $\text{ann}(A_{ij}) \supseteq \text{ann}(A_{ii})$ .

Let  $v \in \text{row}(A) \setminus \{0\}$ , let  $j = \ell(v)$ . Write  $v = \sum_{i=1}^t r_i A_i$  for some  $r_1, \dots, r_t \in R$ . Hence  $v_1 = r_1 A_{1,1} = 0, v_2 = r_1 A_{1,2} + r_2 A_{2,2} = 0, \dots, v_{j-1} = r_1 A_{1,j-1} + \dots + r_{j-1} A_{j-1,j-1}$ . By induction on  $i$  one can show that  $r_i A_{ii} = 0$  for  $1 \leq i < j$ , hence  $r_i A_i = 0$  for  $1 \leq i < j$ . Therefore  $v = \sum_{i=j}^t r_i A_i \in \langle A_j, \dots, A_t \rangle$ , so  $A$  is in reduced row-echelon form according to Definition 10.  $\square$

We conclude this section with Proposition 32, that shows that the error-trapping decoding scheme proposed in [4] for the MAMC can be interpreted as a minimum distance decoding with respect to the distance function from Definition 20. Before stating our result, we recall the scheme of [4, Section IX].

**Example 31** (Error-trapping decoding). Let  $R$  be a finite chain ring. Fix  $N$  such that  $n \geq 2N$  and consider the channel equation  $Y = AX + Z$ , where  $A \in R^{N \times t}$  is left-invertible,  $X \in R^{t \times n}$  is the matrix whose rows generate the transmitted module, and  $Z \in R^{N \times n}$  is a noise matrix whose row-module is isomorphic to  $R^v$  for some integer  $v \leq N$ . One can write

$$A = P \begin{bmatrix} 0_{(N-t) \times t} \\ I_t \end{bmatrix},$$

where  $P \in R^{N \times N}$  is an invertible matrix. Fix  $u \geq v$ . If  $t + v > N$  let  $X \in R^{t \times n}$  be of the form

$$X = \begin{bmatrix} 0 & 0 \\ 0 & \overline{X} \end{bmatrix},$$

where  $\overline{X}$  is a matrix in principal form of size  $(N - u) \times (n - u)$ . If  $t + v \leq N$  let  $X \in R^{t \times n}$  be of the form

$$X = \begin{bmatrix} 0 & \overline{X} \end{bmatrix},$$

where  $\overline{X}$  is a matrix in principal form of size  $t \times (n - u)$ . Under the assumption that error trapping is successful, [4, Section IX.B] shows that the row canonical form of  $Y = AX + Z$  is

$$\begin{bmatrix} Z_1 & Z_2 \\ 0 & \overline{X} \\ 0 & 0 \end{bmatrix},$$

for suitable matrices  $Z_1 \in R^{v \times u}$  and  $Z_2 \in R^{v \times (n-u)}$ . Hence  $\overline{X}$  and  $X$  can be obtained by computing the row canonical form of  $Y$ .

In some cases, the error-trapping decoding from [4] can be seen as an instance of minimum distance decoding according to our definition. Notice that the choice  $u = v$  is particularly interesting, since it maximizes the number of codewords for the given channel, without affecting the error-correction capability of the code.

**Proposition 32.** Following the notation of Example 31, and under the assumption that either  $t + v = N$  or  $u = v$  and  $t + v > N$ , we have

$$d\left(\text{row}(Y), \text{row}\begin{bmatrix} 0 & 0 \\ 0 & \overline{T} \end{bmatrix}\right) \geq d\left(\text{row}(Y), \text{row}\begin{bmatrix} 0 & 0 \\ 0 & \overline{X} \end{bmatrix}\right)$$

for any principal matrix in row canonical form  $\overline{T}$  of the same size as  $\overline{X}$ . Moreover, equality holds if and only if  $\overline{T} = \overline{X}$ .

*Proof.* Since error-trapping is successful, by [4, Section IX.B] there exist matrices  $G, H, K$  such that

$$Y = G \cdot \begin{bmatrix} H & K \\ 0 & \overline{X} \end{bmatrix},$$

where  $G \in R^{N \times N}$  is invertible,  $H \in R^{v \times u}$  and  $\text{row}(H) \cong R^v$ ,  $K \in R^{v \times (n-u)}$ . Since  $\text{row}(H) \cong R^v$ ,

$$\text{row}\begin{bmatrix} H & K \\ 0 & \overline{X} \end{bmatrix} \cap \text{row}\begin{bmatrix} 0 & 0 \\ 0 & \overline{T} \end{bmatrix} = \text{row}\begin{bmatrix} 0 & 0 \\ 0 & \overline{X} \end{bmatrix} \cap \text{row}\begin{bmatrix} 0 & 0 \\ 0 & \overline{T} \end{bmatrix}.$$

Therefore

$$\begin{aligned} d\left(\text{row}(Y), \text{row}\begin{bmatrix} 0 & 0 \\ 0 & \overline{T} \end{bmatrix}\right) &= \lambda(\text{row}(Y)) + \lambda(\text{row}(\overline{T})) - 2\lambda(\text{row}(\overline{X}) \cap \text{row}(\overline{T})) \\ &= d\left(\text{row}(Y), \text{row}\begin{bmatrix} 0 & 0 \\ 0 & \overline{X} \end{bmatrix}\right) + \lambda(\text{row}(\overline{T})) + \lambda(\text{row}(\overline{X})) - 2\lambda(\text{row}(\overline{X}) \cap \text{row}(\overline{T})) \\ &= d\left(\text{row}(Y), \text{row}\begin{bmatrix} 0 & 0 \\ 0 & \overline{X} \end{bmatrix}\right) + d\left(\text{row}\begin{bmatrix} 0 & 0 \\ 0 & \overline{X} \end{bmatrix}, \text{row}\begin{bmatrix} 0 & 0 \\ 0 & \overline{T} \end{bmatrix}\right). \end{aligned}$$

The result now follows from the fact that both  $\overline{X}$  and  $\overline{T}$  are principal matrices in row canonical form, hence they are in reduced row-echelon form by Proposition 30.  $\square$

## 4 Bounds

In this section we derive two upper-bounds on the cardinality of a submodule code with given minimum distance. We also discuss in detail some choices of rings or of the code parameters, for which our bound can be made more precise.

As in the previous sections, we fix a finite PIR  $R$ , an  $R$ -module  $\Omega \subseteq R^n$  of the form (2), and let  $\mathcal{M}(\Omega)$  denote the set of  $R$ -submodules of  $\Omega$ .

**Notation 33.** For  $M \in \mathcal{M}(\Omega)$  and  $1 \leq s \leq \lambda(M)$  let

$$\begin{bmatrix} M \\ s \end{bmatrix}_R = |\{N \in \mathcal{M}(M) : \lambda(N) = s\}|.$$

For  $1 \leq s \leq \lambda$  let

$$\begin{bmatrix} \lambda \\ s \end{bmatrix}_R = \min \left\{ \begin{bmatrix} M \\ s \end{bmatrix}_R : M \in \mathcal{M}(\Omega), \lambda(M) = \lambda \right\}.$$

When there is no ambiguity, we omit the subscript  $R$ . Moreover, we denote by

$$\begin{bmatrix} \lambda \\ s \end{bmatrix}_q = \begin{bmatrix} \lambda \\ s \end{bmatrix}_{\mathbb{F}_q}$$

the  $q$ -ary binomial coefficient.

We restrict our attention to submodule codes  $\mathcal{C} \subseteq \mathcal{M}(\Omega)$  where all codewords have the same length  $k$ ,  $1 \leq k \leq n \cdot \lambda(R) - 1$ . Submodule codes of this kind have even minimum distance, and they are the module-analogue of constant-dimension subspace codes. The next result is a natural extension to submodule codes of the Singleton-like bound for subspace codes.

**Theorem 34.** Let  $\mathcal{C} \subseteq \mathcal{M}(\Omega)$  be a submodule code with  $\lambda(M) = k$  for all  $M \in \mathcal{C}$  and minimum distance  $d(\mathcal{C}) = 2\delta$ . Then

$$|\mathcal{C}| \leq \begin{bmatrix} \lambda(\Omega) - \delta + 1 \\ k - \delta + 1 \end{bmatrix}.$$

*Proof.* Let  $M \in \mathcal{M}(\Omega)$  be an  $R$ -module with  $\lambda(M) = \lambda(\Omega) - \delta + 1$ . By Lemma 6, for all  $N \in \mathcal{C}$

$$\lambda(M \cap N) = \lambda(M) + \lambda(N) - \lambda(M + N) \geq \lambda(\Omega) - \delta + 1 + k - \lambda(\Omega) = k - \delta + 1.$$

For every  $N \in \mathcal{C}$  choose an  $R$ -submodule  $N' \subseteq M \cap N$  with  $\lambda(N') = k - \delta + 1$ . For any  $N, P \in \mathcal{C}$  with  $N \neq P$  we have  $2\delta = d(\mathcal{C}) \leq d(N, P) = 2k - 2\lambda(N \cap P)$ , hence  $\lambda(N \cap P) \leq k - \delta$ . Hence

$$d(N', P') = 2(k - \delta + 1) - 2\lambda(N' \cap P') \geq 2(k - \delta + 1) - 2(k - \delta) = 2,$$

in particular  $N' \neq P'$ . It follows that  $\mathcal{C}' = \{N' : N \in \mathcal{C}\}$  is a set of submodules of  $M$  of length  $k - \delta + 1$  with  $|\mathcal{C}'| = |\mathcal{C}|$ . Therefore

$$|\mathcal{C}| = |\mathcal{C}'| \leq \begin{bmatrix} M \\ k - \delta + 1 \end{bmatrix},$$

for any  $M \in \mathcal{M}(\Omega)$  of length  $\lambda(\Omega) - \delta + 1$ . □

**Remark 35.** For a given  $R$  and fixed  $m, \ell$ , the quantity  $\begin{bmatrix} M \\ \ell \end{bmatrix}$  may depend on the choice of  $M$  of length  $m$ . E.g., let  $R = \mathbb{Z}_5[i] \supseteq I = (2 + i)$  and  $\Omega = R^2$ . Then  $R \times 0$  and  $I \times I$  are two  $R$ -modules of length 2. The ideals of length one of  $R$  are exactly  $I = (2 + i)$  and  $(2 - i)$ , while  $I \times I$  contains at least three submodules of length one, namely  $I \times 0, 0 \times I$ , and  $(1, 1)I = \langle (2 + i, 2 + i) \rangle$ .

**Remark 36.** Since every  $R$ -module of length greater than or equal to  $\lambda(\Omega) - \delta + 1$  contains an  $R$ -submodule of length  $\lambda(\Omega) - \delta + 1$ , the bound of Theorem 34 can also be stated as

$$|\mathcal{C}| \leq \min \left\{ \begin{bmatrix} M \\ k - \delta + 1 \end{bmatrix} : M \in \mathcal{M}(\Omega), \lambda(M) \geq \lambda(\Omega) - \delta + 1 \right\}.$$

The following is another simple bound for the cardinality of a submodule code.

**Theorem 37.** Let  $\mathcal{C} \subseteq \mathcal{M}(\Omega)$  be a submodule code with  $\lambda(M) = k$  for all  $M \in \mathcal{C}$ , and minimum distance  $d(\mathcal{C}) = 2\delta$ . Then

$$|\mathcal{C}| \leq \frac{\begin{bmatrix} \Omega \\ k - \delta + 1 \end{bmatrix}}{\begin{bmatrix} k \\ k - \delta + 1 \end{bmatrix}}.$$

*Proof.* Each  $M \in \mathcal{C}$  contains at least  $\begin{bmatrix} k \\ k - \delta + 1 \end{bmatrix}$  submodules of  $\Omega$  of length  $k - \delta + 1$ . Moreover, a submodule of  $\Omega$  of length  $k - \delta + 1$  cannot be contained in two distinct  $M, N \in \mathcal{C}$ , as otherwise  $\lambda(M \cap N) \geq k - \delta + 1$ , hence  $d(M, N) < 2\delta$ . Therefore

$$\begin{bmatrix} \Omega \\ k - \delta + 1 \end{bmatrix} \geq |\mathcal{C}| \cdot \begin{bmatrix} k \\ k - \delta + 1 \end{bmatrix},$$

which proves the bound.  $\square$

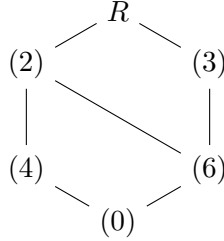
**Remark 38.** The upper bounds of Theorem 34 and 37 are not comparable. For example, let  $k = \delta$ ,  $R = \mathbb{F}_q$ , and  $\Omega = \mathbb{F}_q^n$ . Assume that  $k \mid n$ . The bound of Theorem 34 is

$$|\mathcal{C}| \leq \begin{bmatrix} n - k + 1 \\ 1 \end{bmatrix}_q = q^{n-k} + q^{n-k-1} + \dots + q + 1,$$

while the bound of Theorem 37 is

$$|\mathcal{C}| \leq \frac{\begin{bmatrix} n \\ 1 \end{bmatrix}_q}{\begin{bmatrix} k \\ 1 \end{bmatrix}_q} = \frac{q^n - 1}{q^k - 1} = q^{n-k} + q^{n-2k} + \dots + q^k + 1.$$

However, one can also find examples in which Theorem 34 yields a better bound than Theorem 37. E.g., let  $R = \mathbb{Z}_{12}$ . The Hasse diagram of the ideals of  $R$  is



In particular,  $\lambda(R) = 3$ . Let  $\Omega = R^2$  and let  $\mathcal{C} \subseteq \mathcal{M}(\Omega)$  be a submodule code with  $k = \delta = 2$ . By Theorem 25, the module

$$M = \text{row} \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix} \subseteq \Omega$$

has  $\lambda(M) = \lambda(1) + \lambda(3) = 5$ . Moreover, the submodules of  $M$  of length 1 are precisely those generated by one of the following vectors:  $(4, 0), (6, 0), (6, 6), (0, 6)$ . Therefore,  $|\mathcal{C}| \leq 4$  by Theorem 34. Now let  $N = \langle (0, 3) \rangle \subseteq \Omega$ . Then  $\lambda(N) = 2$  and  $N$  has a unique submodule of length 1, namely  $\langle (0, 6) \rangle$ . Hence

$$\begin{bmatrix} 2 \\ 1 \end{bmatrix} = \min \left\{ \begin{bmatrix} N \\ 1 \end{bmatrix} : N \in \mathcal{M}(\Omega), \lambda(N) = 2 \right\} = 1.$$

One can check that the submodules of  $\Omega$  of length 1 are exactly those generated by one of the following vectors:  $(4, 0), (4, 4), (4, 8), (6, 0), (6, 6), (0, 4), (0, 6)$ . Therefore the bound of Theorem 37 reads

$$|\mathcal{C}| \leq \begin{bmatrix} \Omega \\ 1 \end{bmatrix} / \begin{bmatrix} 2 \\ 1 \end{bmatrix} = 7 > 4.$$

The bounds of Theorem 34 and Theorem 37 can be made more explicit for PIR's which are isomorphic to  $\mathbb{Z}_p^m$  for some  $m \geq 1$ . An example of such ring is  $\mathbb{Z}_p[i]$ , which is isomorphic to  $\mathbb{Z}_p^2$  if  $p \equiv 1 \pmod{4}$ , as we show next. Notice that in the other cases  $\mathbb{Z}_p[i]$  is either a finite chain ring or a finite field.

**Remark 39.** Let  $p$  be a prime. Then

$$\mathbb{Z}_p[i] \cong \mathbb{Z}_p[x]/(x^2 + 1) \cong \begin{cases} \mathbb{Z}_2[x]/(x+1)^2 & \text{if } p = 2, \\ \mathbb{F}_{p^2} & \text{if } p \equiv 3 \pmod{4}, \\ \mathbb{Z}_p \times \mathbb{Z}_p & \text{if } p \equiv 1 \pmod{4}. \end{cases}$$

Indeed, if  $p = 2$ , then  $x^2 + 1 = (x+1)^2$ . If  $p$  is an odd prime, then  $x^2 + 1$  is reducible if and only if  $-1$  is a quadratic residue modulo  $p$ , if and only if  $p \equiv 1 \pmod{4}$ . The thesis now follows from the Chinese Remainder Theorem.

We start with a preliminary result on the structure of rings of the form  $R \cong \mathbb{Z}_p^m$ .

**Lemma 40.** Let  $R \cong \mathbb{Z}_p^m$ . Then there exist  $e_1, \dots, e_m \in R$  such that

$$R = (e_1) \oplus \dots \oplus (e_m)$$

and  $e_1 + \dots + e_m = 1$ ,  $e_i^2 = e_i$  for all  $1 \leq i \leq m$ , and  $e_i e_j = 0$  if  $i \neq j$ . Moreover,  $\lambda(R) = m$ .

*Proof.* Fix an isomorphism  $\pi : R \rightarrow \mathbb{Z}_p^m$  between  $R$  and  $\mathbb{Z}_p^m$ . Let  $e_i \in R$  be the inverse image via  $\pi$  of the  $i$ -th element of the standard basis of  $\mathbb{Z}_p^m$ . Then  $e_1 + \dots + e_m = 1$ ,  $e_i^2 = e_i$  for all  $1 \leq i \leq m$ , and  $e_i e_j = 0$  if  $i \neq j$ . Notice that  $R$  is a  $\mathbb{Z}_p$ -vector space via  $\alpha r = \pi^{-1}(\alpha \pi(r))$  for  $\alpha \in \mathbb{Z}_p, r \in R$ . This corresponds to identifying  $\mathbb{Z}_p$  with  $\{\pi^{-1}(\alpha, \dots, \alpha) : \alpha \in \mathbb{Z}_p\} \subseteq R$ . Since  $R = (e_1) \oplus \dots \oplus (e_m)$ , then every  $r \in R$  can be written uniquely as  $r = r_1 e_1 + \dots + r_m e_m$  with  $r_i \in \mathbb{Z}_p$ , where we regard  $\mathbb{Z}_p$  as a subset of  $R$  via the identification above. Therefore  $\lambda(R) = m$  and a composition series for  $R$  is given by  $0 \subsetneq (e_1) \subsetneq (e_1, e_2) \subsetneq \dots \subsetneq (e_1, \dots, e_m) = R$ .  $\square$

Using the notation of Lemma 40, we can count the number of submodules of fixed length of any given  $R$ -module  $M$ . For the sake of concreteness we limit our attention to submodules of  $R^n$ , but the same proof applies to any finitely generated  $R$ -module  $M$ .

**Theorem 41.** Let  $R \cong \mathbb{Z}_p^m$ , let  $M \in \mathcal{M}(R^n)$ . The number of  $R$ -submodules of  $M$  of length  $\ell$  is

$$\begin{bmatrix} M \\ \ell \end{bmatrix} = \sum_{\substack{(\ell_1, \dots, \ell_m) \in \mathbb{N}^m, \\ \ell_1 + \dots + \ell_m = \ell}} \prod_{i=1}^m \begin{bmatrix} \dim(e_i M) \\ \ell_i \end{bmatrix}_p.$$

In particular,

$$\begin{bmatrix} M \\ 1 \end{bmatrix} = \sum_{i=1}^m \frac{p^{\dim(e_i M)} - 1}{p - 1}.$$

*Proof.* By Lemma 40, for all  $M \in \mathcal{M}(R^n)$  one has

$$M = e_1 M \oplus \dots \oplus e_m M.$$

Therefore  $\lambda(M) = \sum_{i=1}^m \lambda(e_i M)$ . Moreover, for all  $r = r_1 e_1 + \dots + r_m e_m \in R$  and  $v \in M$  we have  $r e_i v = r_i e_i v$  for all  $i$ . Therefore the  $R$ -submodules of  $e_i M$  coincide with its  $\mathbb{Z}_p$ -subspaces, hence  $\lambda(e_i M) = \dim_{\mathbb{Z}_p}(e_i M)$ . Hence we have shown that for every  $R$ -module  $M \subseteq R^n$

$$\lambda(M) = \sum_{i=1}^m \dim_{\mathbb{Z}_p}(e_i M) = \dim_{\mathbb{Z}_p}(M).$$



Since for every collection of submodules  $N_i \subseteq e_i M$  the module  $N = N_1 \oplus \dots \oplus N_m \in \mathcal{M}(M)$  and the  $R$ -submodules of  $e_i M$  coincide with its  $\mathbb{Z}_p$ -subspaces, then the number of  $R$ -submodules of  $M$  of length  $\ell$  is

$$\begin{bmatrix} M \\ \ell \end{bmatrix} = \sum_{\substack{(\ell_1, \dots, \ell_m) \in \mathbb{N}^m, \\ \ell_1 + \dots + \ell_m = \ell}} \prod_{i=1}^m \begin{bmatrix} \dim(e_i M) \\ \ell_i \end{bmatrix}_p.$$

□

Theorem 41 allows us to evaluate the bounds of Theorem 34 and Theorem 37 as follows.

**Corollary 42.** Let  $R \cong \mathbb{Z}_p^m$ . Let  $\mathcal{C} \subseteq \mathcal{M}(\Omega)$  be a submodule code with  $\lambda(M) = k$  for all  $M \in \mathcal{C}$  and  $d(\mathcal{C}) = 2\delta$ . Let

$$b(\lambda, k, \delta) = \min \left\{ \sum_{\substack{(\ell_1, \dots, \ell_m) \in \mathbb{N}^m, \\ \ell_1 + \dots + \ell_m = k - \delta + 1}} \prod_{i=1}^m \begin{bmatrix} u_i \\ \ell_i \end{bmatrix}_p : (u_1, \dots, u_m) \in \mathbb{N}^m, u_1 + \dots + u_m = \lambda - \delta + 1 \right\}.$$

Then

$$|\mathcal{C}| \leq b(\lambda(\Omega), k, \delta). \quad (4)$$

Moreover,

$$|\mathcal{C}| \leq \frac{\sum_{\substack{(\ell_1, \dots, \ell_m) \in \mathbb{N}^m, \\ \ell_1 + \dots + \ell_m = k - \delta + 1}} \prod_{i=1}^m \begin{bmatrix} \dim(e_i \Omega) \\ \ell_i \end{bmatrix}_p}{b(k + \delta - 1, k, \delta)}. \quad (5)$$

If  $\Omega = R^n$  and  $\delta = k$ , then

$$|\mathcal{C}| \leq \frac{(p^n - 1)/(p - 1)}{\lceil (p^{k/m} - 1)/(p - 1) \rceil}. \quad (6)$$

If in addition  $m = 2$  and  $k$  is odd, then

$$|\mathcal{C}| \leq \lfloor 2(p^n - 1)/(p^h + p^{h-1} - 2) \rfloor, \quad (7)$$

where  $h = \lceil k/2 \rceil$ .

*Proof.* Let  $M \in \mathcal{M}(\Omega)$  be a submodule of length  $\lambda(M) = \lambda(\Omega) - \delta + 1$  and let  $u_i = \dim(e_i M)$  for all  $i$ . By Theorem 41, the number of submodules of  $M$  of length  $k - \delta + 1$  equals

$$\begin{bmatrix} M \\ k - \delta + 1 \end{bmatrix} = \sum_{\substack{(\ell_1, \dots, \ell_m) \in \mathbb{N}^m, \\ \ell_1 + \dots + \ell_m = k - \delta + 1}} \prod_{i=1}^m \begin{bmatrix} u_i \\ \ell_i \end{bmatrix}_p.$$

Hence Theorem 34 implies bound (4). Similarly, bound (5) follows from Theorem 37.

Now assume  $\delta = k$  and  $\Omega = R^n$ . We have

$$b(2k - 1, k, k) = \min \left\{ \frac{1}{p - 1} \left( \sum_{i=1}^m p^{u_i} - m \right) : (u_1, \dots, u_m) \in \mathbb{N}^m, \sum_{i=1}^m u_i = k \right\}.$$

Let  $f : \mathbb{R}^m \rightarrow \mathbb{R}$  be the function defined by  $f(x_1, \dots, x_m) = \sum_{i=1}^m p^{x_i}$  for all  $(x_1, \dots, x_m) \in \mathbb{R}^m$ . Using e.g. the method of Lagrange multipliers from Calculus, one can show that the minimum of  $f$  in the region of  $\mathbb{R}^m$  defined by the constraints

$$\sum_{i=1}^m x_i = k, \quad x_i \geq 0 \text{ for all } i \in \{1, \dots, m\}$$

is attained for  $x_1 = x_2 = \dots = x_m = k/m$ , and that its value is  $mp^{k/m}$ . This shows that

$$b(2k-1, k, k) \geq \lceil (mp^{k/m} - m)/(p-1) \rceil.$$

Bound (6) now follows from bound (5) and the fact that  $\dim(e_i\Omega) = n$  for all  $i \in \{1, \dots, m\}$ . If in addition  $m = 2$  and  $k$  is odd, then without loss of generality we may assume  $u_1 \geq u_2 + 1$ . Using elementary methods from Calculus, one shows that

$$b(2k-1, k, k) \geq \frac{p^h + p^{h-1} - 2}{p-1},$$

where  $h = \lceil k/2 \rceil$ . This concludes the proof.  $\square$

We conclude this section by evaluating the bound of Theorem 34 for finite chain rings. We concentrate on codes  $\mathcal{C} \subseteq \mathcal{M}(\Omega)$  with  $\lambda(M) = k$  for all  $M \in \mathcal{C}$  and  $d(\mathcal{C}) = 2k$ .

**Theorem 43.** Let  $R$  be a finite chain ring of length  $e$ , let  $\pi \in R$  be a generator of the maximal ideal of  $R$ , let  $q$  be the cardinality of the residue field of  $R$ . Let

$$\Omega = R \times (\pi^{a_2}) \times \dots \times (\pi^{a_n})$$

for some  $0 \leq a_2 \leq \dots \leq a_n \leq e-1$ . Let  $\mathcal{C} \subseteq \mathcal{M}(\Omega)$  be a submodule code with  $d(\mathcal{C}) = 2k$  and whose codewords have length  $k$ . Then

$$|\mathcal{C}| \leq \frac{q^m - 1}{q - 1}$$

where  $m = \min\{1 \leq i \leq n \mid (n-i)e - a_{i+1} - \dots - a_n \leq k-1\}$ . In particular, if  $\Omega = R^n$ , then

$$|\mathcal{C}| \leq \frac{q^{n-h+1} - 1}{q - 1}$$

where  $k = he - r$  with  $0 \leq r \leq e-1$ .

*Proof.* We claim that the submodules of length one of an  $R$ -module  $M \subseteq R^n$  are in bijection with the vectors  $v \in M$  of the form

$$v = (\underbrace{0, \dots, 0}_{i-1}, \pi^{e-1}, v_{i+1}, \dots, v_n) \quad (8)$$

where  $1 \leq i \leq n$  and  $v_{i+1}, \dots, v_n \in (\pi^{e-1})$ . In fact, every module of length one is minimally generated by one vector. If we represent a module generated by one vector by a matrix in reduced row-echelon form, then such a matrix has a unique row by Theorem 25, and by Proposition 17 the row is of the form  $v = (0, \dots, 0, \pi^s, v_{i+1}, \dots, v_n)$  with  $v_{i+1}, \dots, v_n \in (\pi^s)$ . Finally,  $\lambda(\langle v \rangle) = \lambda(\pi^s) = e - s$  by Theorem 25. Hence the modules of length one are exactly those generated by vectors of the form (8). By uniqueness of the reduced row-echelon form, two such modules are distinct if and only if they are generated by distinct vectors in reduced row-echelon form. This proves the claim. Notice that there are exactly  $q^{n-i}$  vectors of the form (8), for a fixed  $i \in \{1, \dots, n\}$ .

Let  $M \subseteq \Omega$  be a submodule of length  $\lambda(\Omega) - k + 1$ . Let  $m$  be the least integer such that

$$M \subseteq R^m \times \underbrace{0 \times \dots \times 0}_{n-m}.$$

Notice that  $m$  depends on  $M$ , and not just on its length. Then  $M$  contains exactly  $q^{m-1} + q^{m-2} + \dots + q + 1 = \frac{q^m - 1}{q - 1}$  vectors of the form (8), since each such vector has  $v_{i+1}, \dots, v_m \in (\pi^{e-1})$

and  $v_{m+1} = \dots = v_n = 0$ , for some  $1 \leq i \leq m$ . Since  $\Omega = R \times (\pi^{a_2}) \times \dots \times (\pi^{a_n})$ , then  $\lambda(\Omega) = ne - a_2 - \dots - a_n$ . If

$$M \subseteq (R^i \times 0 \times \dots \times 0) \cap \Omega = R \times \pi^{a_2} R \times \dots \times \pi^{a_i} R \times 0 \times \dots \times 0$$

for some  $i$ , then  $\lambda(M) = ne - a_2 - \dots - a_n - k + 1 \leq \lambda(R \times \pi^{a_2} R \times \dots \times \pi^{a_i} R) = ie - a_2 - \dots - a_i$ . Hence

$$m \geq \min\{1 \leq i \leq n : (n-i)e - a_{i+1} - \dots - a_n \leq k-1\}$$

and equality holds for any  $M \subseteq R \times (\pi^{a_2}) \times \dots \times (\pi^{a_m}) \times 0 \times \dots \times 0$ . By Theorem 34

$$\begin{aligned} |\mathcal{C}| &\leq \min \left\{ \left\lceil \frac{M}{k-\delta+1} \right\rceil : M \subseteq \Omega, \lambda(M) = \lambda(\Omega) - \delta + 1 \right\} \\ &= \min \left\{ \frac{q^i - 1}{q - 1} : M \subseteq \Omega \cap R^i \times 0 \times \dots \times 0, \lambda(M) = \lambda(\Omega) - \delta + 1 \right\} = \frac{q^m - 1}{q - 1} \end{aligned}$$

where  $m = \min\{1 \leq i \leq n \mid (n-i)e - a_{i+1} - \dots - a_n \leq k-1\}$ .

If  $\Omega = R^n$ , then  $a_2 = \dots = a_n = 0$ . Write  $k = he - r$  with  $0 \leq r \leq e-1$ . Then  $(h-1)e \leq k-1 \leq he-1$ , hence  $m = \min\{1 \leq i \leq n \mid (n-i)e \leq k-1\} = n-h+1$ .  $\square$

## 5 Constructions

In this section we propose some constructions for submodule codes for an ambient space of the form  $\Omega = R^n$ . Throughout the section we say that a code is asymptotically optimal if its cardinality asymptotically meets one of the bounds of the previous section. We say that a code is optimal if its cardinality exactly meets one of the bounds.

We first concentrate on finite chain rings, and show how to construct optimal codes of maximum correction capability. Our codes can be regarded as the submodule code analogue of the partial spread codes from [6]. We then look at finite PIR's that contain a field  $\mathbb{F}$ , and show how subspace codes over  $\mathbb{F}$  can be lifted to submodule codes over  $R$  by tensoring them with  $R$ . This allows us to construct optimal submodule codes over  $\mathbb{Z}_p[i]$  of maximum correction capability. Finally we show how to obtain submodule codes over a ring of the form  $R_1 \times \dots \times R_m$  from submodule codes over  $R_1, \dots, R_m$ . We propose two constructions of the latter type, and discuss their decoding. For the first construction we take a cartesian product of codes on the  $R_i$ 's and show that this yields a code on  $R$ , whose parameters are determined and whose decoding can be reduced to decoding on each of the  $R_i$ 's. However, not every code over a  $R$  is a product of codes over the  $R_i$ 's: Our second construction yields a code over  $R$  which is not a product. We show that, in that case, decoding cannot be reduced to decoding on each of the  $R_i$ 's. This shows in particular that, although every finite PIR  $R$  is isomorphic to a product of finite fields and finite chain rings, the study of codes over  $R$  cannot be reduced in general to the study of codes over finite fields and finite chain rings.

### 5.1 Partial spreads over finite chain rings

We start with a construction that can be applied to any PIR. Its optimality relies on the existence of large sets of matrices, in which the length of the difference of any two of them is maximum. In Proposition 46 we will show that such large sets can be constructed over any finite chain ring.

**Theorem 44.** Let  $R$  be a finite PIR. Let  $n, k$  be positive integers. Write  $k = h \cdot \lambda(R) - r$  with  $0 \leq r \leq \lambda(R) - 1$ , and assume  $n \geq 2h$ . Write  $n = \nu \cdot h + \rho$  with  $0 \leq \rho \leq h-1$ . Let  $\mathcal{A} \subseteq R^{h \times h}$  and

$\mathcal{A}' \subseteq R^{h \times (h+\rho)}$  be subsets such that  $\lambda(\text{row}(A - B)) = h \cdot \lambda(R)$  for all  $A, B \in \mathcal{A}$  with  $A \neq B$  and  $A, B \in \mathcal{A}'$  with  $A \neq B$ . For  $i \in \{1, \dots, \nu - 1\}$  let

$$\mathcal{S}_i = \left\{ \begin{bmatrix} 0_{h \times h} & \dots & 0_{h \times h} & I_{h \times h} & A_{i+1} & \dots & A_{\nu-1} & A_\nu \end{bmatrix} : A_{i+1}, \dots, A_{\nu-1} \in \mathcal{A}, A_\nu \in \mathcal{A}' \right\} \subseteq R^{h \times n},$$

where  $I_{h \times h}$  is the identity matrix of size  $h \times h$ . Define  $\mathcal{S}_\nu = \left\{ \begin{bmatrix} 0_{h \times (n-h)} & I_{h \times h} \end{bmatrix} \right\}$ . Let  $\zeta \in R$  generate an ideal of length  $\lambda(R) - r$ . For all  $i \in \{1, \dots, \nu\}$  let

$$\mathcal{S}_{i,\zeta} = \{M_\zeta : M \in \mathcal{S}_i\},$$

where  $M_\zeta$  is the matrix obtained from  $M$  by multiplying its last row by  $\zeta$ . Then

$$\mathcal{C} = \bigcup_{i=1}^{\nu} \{\text{row}(M) : M \in \mathcal{S}_{i,\zeta}\}$$

is a submodule code of length  $\lambda(\mathcal{C}) = k$ , minimum distance  $d(\mathcal{C}) = 2k$ , and cardinality

$$|\mathcal{C}| = |\mathcal{A}'| \cdot \frac{|\mathcal{A}|^{\nu-1} - 1}{|\mathcal{A}| - 1} + 1.$$

*Proof.* Let  $M_\zeta \in \mathcal{S}_{i,\zeta}$ . Then  $M_\zeta$  is in row-echelon form and  $\lambda(\text{row}(M_\zeta)) = (h-1) \cdot \lambda(R) + \lambda(\zeta) = k$  by Theorem 25. Define the code

$$\mathcal{C}' = \bigcup_{i=1}^{\nu} \{\text{row}(M) : M \in \mathcal{S}_i\}.$$

Again  $M$  is in row-echelon form and  $\lambda(\text{row}(M)) = h \cdot \lambda(R)$ . Moreover, arguing as in [6, Theorem 13 and Proposition 17] and replacing the rank with the length, one sees that  $d(\mathcal{C}') = 2h \cdot \lambda(R)$ , i.e., the submodules that constitute  $\mathcal{C}'$  have trivial pairwise intersections. Moreover,

$$|\mathcal{C}'| = |\mathcal{A}'| \cdot \frac{|\mathcal{A}|^{\nu-1} - 1}{|\mathcal{A}| - 1} + 1.$$

Now observe that  $\mathcal{C}$  is obtained from  $\mathcal{C}'$  by taking an appropriate submodule of each codeword. Therefore the codewords of  $\mathcal{C}$  have trivial pairwise intersection. Hence  $d(\mathcal{C}) = 2k$  and  $|\mathcal{C}| = |\mathcal{C}'|$ .  $\square$

We now show that over a finite chain ring  $R$  one can construct large sets  $\mathcal{A}$  and  $\mathcal{A}'$  to be used within the construction from Theorem 44.

**Lemma 45.** Let  $R$  be a ring, let  $s, t > 0$ . Then for any  $v_1, \dots, v_t \in R^s$  we have  $\lambda(\langle v_1, \dots, v_t \rangle) \leq t \cdot \lambda(R)$ .

*Proof.* Let  $A \in R^{t \times s}$  be the matrix with rows  $v_1, \dots, v_t$ . Right multiplication by  $A$  induces an  $R$ -homomorphism  $f_A : R^t \rightarrow R^s$ , whose image is  $\langle v_1, \dots, v_t \rangle$ . Since  $\text{Im}(f_A) \cong R^t / \ker(f_A)$ , then  $\lambda(\langle v_1, \dots, v_t \rangle) = \lambda(R^t) - \lambda(\ker(f_A)) \leq \lambda(R^t) = t \cdot \lambda(R)$ .  $\square$

**Proposition 46.** Let  $R$  be a finite chain ring with residue field of order  $q$ . Then for all  $h > 0$  and for all  $0 \leq \rho \leq h-1$  there exists a set  $\mathcal{A} \subseteq R^{h \times (h+\rho)}$  with  $|\mathcal{A}| = q^{h+\rho}$  and  $\lambda(\text{row}(A - B)) = h \cdot \lambda(R)$  for all  $A, B \in \mathcal{A}$  with  $A \neq B$ .

*Proof.* We first prove the statement for  $\rho = 0$ . Let  $\pi$  be a generator of the maximal ideal of  $R$ , and let  $f : R \rightarrow R/(\pi)$  be the projection map. Let  $\iota : R/(\pi) \rightarrow R$  be such that  $f \circ \iota$  is the identity of  $R/(\pi)$ . Such a  $\iota$  can be obtained by mapping each element of  $R/(\pi)$  to one of its representatives in  $R$ . Notice that we do not require that  $\iota$  is a ring homomorphism. We extend  $f$  and  $\iota$  entrywise to  $f : R^{h \times h} \rightarrow (R/(\pi))^{h \times h}$  and  $\iota : (R/(\pi))^{h \times h} \rightarrow R^{h \times h}$ .

Since  $(R/(\pi))^{h \times h} \cong \mathbb{F}_q^{h \times h}$ , by [3, Section 6] there exists  $\mathcal{A}' \subseteq (R/(\pi))^{h \times h}$  with  $|\mathcal{A}'| = q^h$  and  $A' - B'$  invertible for any  $A', B' \in \mathcal{A}'$  with  $A' \neq B'$ . Then the set of matrices  $\mathcal{A} = \{\iota(A') : A' \in \mathcal{A}'\} \subseteq R^{h \times h}$  has the expected properties. Indeed, let  $A', B' \in \mathcal{A}'$  with  $A' \neq B'$ . Since  $f$  is a ring homomorphism, we have

$$f(\det(\iota(A') - \iota(B'))) = \det(f(\iota(A')) - f(\iota(B'))) = \det(A' - B') \neq 0.$$

Therefore  $\det(\iota(A') - \iota(B')) \notin (\pi)$ . As  $(\pi)$  is the only maximal ideal of  $R$ ,  $\det(\iota(A') - \iota(B'))$  is invertible, hence  $\iota(A') - \iota(B')$  is invertible. This implies  $\text{row}(\iota(A') - \iota(B')) \cong R^h$ , which has length  $h \cdot \lambda(R)$ . In addition  $|\mathcal{A}| = |\mathcal{A}'| = q^h$ .

Now assume  $\rho > 0$ , and set  $h' = h + \rho$ . By the first part of the proof there exists a set of matrices  $\mathcal{B} \subseteq R^{h' \times h'}$  with  $\lambda(\text{row}(A - B)) = h' \cdot \lambda(R)$  for all  $A, B \in \mathcal{B}$  with  $A \neq B$ . For  $A \in \mathcal{B}$  denote by  $\overline{A}$  the matrix obtained from  $A$  by deleting the first  $\rho$  rows. A simple application of Lemma 45 shows that the set  $\mathcal{A} = \{\overline{A} : A \in \mathcal{B}\} \subseteq R^{h \times h'}$  has the desired properties.  $\square$

**Example 47.** Let  $R$  be a finite chain ring with residue field of order  $q$ . Following the notation of Theorem 44, Proposition 46 allows us to construct a submodule code  $\mathcal{C} \subseteq \mathcal{M}(R^n)$  of constant length  $\lambda(\mathcal{C}) = k$ , minimum distance  $d(\mathcal{C}) = 2k$ , and cardinality

$$|\mathcal{C}| = q^{h+\rho} \cdot \frac{q^{h(\nu-1)} - 1}{q^h - 1} + 1 = \frac{q^n - q^{h+\rho} + q^h - 1}{q^h - 1} \in \mathcal{O}(q^{n-h})$$

(as  $n > h + \rho$ ). Let  $\overline{\mathcal{C}}$  be a submodule code with the same parameters as  $\mathcal{C}$  and maximum cardinality. By Theorem 43 we have  $|\overline{\mathcal{C}}| \leq (q^{n-h+1} - 1)/(q - 1)$ . Therefore

$$1 \geq \frac{|\mathcal{C}|}{|\overline{\mathcal{C}}|} \geq \frac{q^n - q^{h+\rho} + q^h - 1}{q^h - 1} \cdot \frac{q - 1}{q^{n-h+1} - 1} \xrightarrow{q \rightarrow \infty} 1.$$

This shows that  $\mathcal{C}$  is an asymptotically optimal submodule code.

## 5.2 Tensor product construction and partial spreads over rings of the form $\mathbb{Z}_p^m$

Assume that  $R$  contains a finite field  $\mathbb{F} \subseteq R$  as a subring and that  $R$  and  $\mathbb{F}$  have the same one. Let  $V \subseteq \mathbb{F}^n$  be an  $\mathbb{F}$ -linear space. Recall that the tensor product  $V \otimes_{\mathbb{F}} R \subseteq R^n$  is the submodule of  $R^n$  generated by the elements of  $V$ . If  $V = \langle v_1, \dots, v_m \rangle_{\mathbb{F}}$ , then

$$V \otimes_{\mathbb{F}} R = \langle v : v \in V \rangle_R = \langle v_1, \dots, v_m \rangle_R.$$

**Lemma 48.** Let  $V \subseteq \mathbb{F}^n$  be an  $\mathbb{F}$ -linear space. Then

$$\lambda(V \otimes_{\mathbb{F}} R) = \lambda(R) \cdot \dim_{\mathbb{F}}(V).$$

*Proof.* Let  $t = \dim_{\mathbb{F}}(V)$ , and let  $A \in \mathbb{F}^{t \times n}$  be a matrix in reduced row-echelon form, whose rows generate  $V$ . Regard  $A$  as a matrix over  $R$ . Then  $A$  is still in row-echelon form and  $\text{row}(A) = V \otimes_{\mathbb{F}} R$ . Since all the pivots of  $A$  are ones, by Theorem 25 we have  $\lambda(V \otimes_{\mathbb{F}} R) = \lambda(1) \cdot t = \lambda(R) \cdot \dim_{\mathbb{F}}(V)$ , as claimed.  $\square$

**Lemma 49.** Let  $V, W \subseteq \mathbb{F}^n$  be  $\mathbb{F}$ -linear spaces. Then  $(V \otimes_{\mathbb{F}} R) \cap (W \otimes_{\mathbb{F}} R) = (V \cap W) \otimes_{\mathbb{F}} R$ .

*Proof.* By definition  $(V \cap W) \otimes_{\mathbb{F}} R \subseteq (V \otimes_{\mathbb{F}} R) \cap (W \otimes_{\mathbb{F}} R)$ . Therefore by Lemma 6 it suffices to show that they have the same length. By Lemma 48

$$\begin{aligned} \lambda((V \cap W) \otimes_{\mathbb{F}} R) &= \lambda(R) \cdot \dim_{\mathbb{F}}(V \cap W) = \lambda(R) \cdot (\dim_{\mathbb{F}}(V) + \dim_{\mathbb{F}}(W) - \dim_{\mathbb{F}}(V + W)) = \\ &= \lambda(V \otimes_{\mathbb{F}} R) + \lambda(W \otimes_{\mathbb{F}} R) - \lambda((V + W) \otimes_{\mathbb{F}} R) = \lambda((V \otimes_{\mathbb{F}} R) \cap (W \otimes_{\mathbb{F}} R)), \end{aligned}$$

where the last equality follows from Lemma 6 and from observing that  $(V + W) \otimes_{\mathbb{F}} R = V \otimes_{\mathbb{F}} R + W \otimes_{\mathbb{F}} R$ .  $\square$

From Lemma 48 and 49 one obtains the following construction.

**Theorem 50.** Let  $\mathcal{C} \subseteq \mathcal{M}(\mathbb{F}^n)$  be a subspace code of minimum subspace distance  $2\delta$  and  $\dim_{\mathbb{F}}(V) = k$  for all  $V \in \mathcal{C}$ . Then

$$\mathcal{C} \otimes_{\mathbb{F}} R = \{V \otimes_{\mathbb{F}} R : V \in \mathcal{C}\} \subseteq \mathcal{M}(R^n)$$

is a submodule code of cardinality  $|\mathcal{C} \otimes_{\mathbb{F}} R| = |\mathcal{C}|$ , whose codewords have length  $\lambda(R) \cdot k$ , and whose minimum distance is  $2\lambda(R) \cdot \delta$ .

**Example 51.** Let  $\mathbb{F} = \mathbb{Z}_p$  and  $R = \mathbb{Z}_p^m$ . Then  $\mathbb{Z}_p \cong \{(a, a, \dots, a) : a \in \mathbb{Z}_p\} \subseteq R$  can be viewed as a subring of  $R$ . We have  $\lambda(R) = m$ . Let  $h$  be an integer,  $1 \leq h \leq n/2$ . By [6, Theorem 13 and Proposition 17], there exists a subspace code  $\mathcal{C} \subseteq \mathcal{M}(\mathbb{Z}_p^n)$  of constant dimension  $h$ , minimum distance  $2h$  and cardinality  $(p^n - p^{h+\rho} + p^h - 1)/(p^h - 1)$ , where  $\rho$  is the remainder of the division of  $n$  by  $h$ . By Theorem 50,  $\mathcal{C} \otimes_{\mathbb{Z}_p} R \subseteq \mathcal{M}(R^n)$  is a submodule code whose codewords have length  $mh$  and minimum distance  $2mh$ . Moreover,

$$|\mathcal{C} \otimes_{\mathbb{Z}_p} R| = \frac{p^n - p^\rho}{p^h - 1} - p^\rho + 1.$$

Let  $\overline{\mathcal{C}}$  be a submodule code with the same parameters as  $\mathcal{C} \otimes_{\mathbb{Z}_p} R$  and maximum cardinality. By Theorem 42 (6),  $|\overline{\mathcal{C}}| \leq (p^n - 1)/(p^h - 1)$ . Therefore

$$1 \geq \frac{|\mathcal{C} \otimes_{\mathbb{Z}_p} R|}{|\overline{\mathcal{C}}|} \geq \frac{p^n - p^{h+\rho} + p^h - 1}{p^h - 1} \cdot \frac{p^h - 1}{p^n - 1} \xrightarrow{q \rightarrow \infty} 1.$$

Hence  $\mathcal{C} \otimes_{\mathbb{Z}_p} R$  is asymptotically optimal, and it is optimal when  $\rho = 0$ .

Fix  $1 \leq \ell \leq m - 1$ . For all  $M \in \mathcal{C} \otimes_{\mathbb{Z}_p} R$  choose a submodule  $M' \subseteq M$  with  $\lambda(M') = mh - \ell$ . Then  $\mathcal{D} = \{M' : M \in \mathcal{C} \otimes_{\mathbb{Z}_p} R\} \subseteq \mathcal{M}(R^n)$  is a submodule code with minimum distance  $2mh - 2\ell$  and whose codewords have length  $mh - \ell$ . Moreover,

$$|\mathcal{D}| = |\mathcal{C} \otimes_{\mathbb{Z}_p} R| = \frac{p^n - p^\rho}{p^h - 1} - p^\rho + 1.$$

Let  $\overline{\mathcal{D}}$  be a submodule code with the same parameters as  $\mathcal{D}$  and maximum cardinality. By Theorem 42 (6) we have  $|\overline{\mathcal{D}}| \leq (p^n - 1)/(p^{h-\ell/m} - 1)$ . Therefore

$$1 \geq \frac{|\mathcal{D}|}{|\overline{\mathcal{D}}|} \geq \frac{p^n - p^{h+\rho} + p^h - 1}{p^h - 1} \cdot \frac{p^{h-\ell/m} - 1}{p^n - 1} \in \mathcal{O}(p^{-\ell/m}).$$

If in addition  $m = 2$ , then by Proposition 42 (7)

$$1 \geq \frac{|\mathcal{D}|}{|\overline{\mathcal{D}}|} \geq \frac{p^n - p^{h+\rho} + p^h - 1}{p^h - 1} \cdot \frac{p^h + p^{h-1} - 2}{2(p^n - 1)} \xrightarrow{q \rightarrow \infty} 1/2.$$

Therefore  $\mathcal{D}$  is asymptotically optimal, up to a factor 2.

**Remark 52.** Let  $\mathcal{C} \subseteq \mathcal{M}(\mathbb{F}^n)$  be a subspace code over the finite field  $\mathbb{F}$ , and let  $W \subseteq \mathbb{F}^n$  be a decodable space for the code  $\mathcal{C}$ , i.e., an  $\mathbb{F}$ -linear space for which there exists  $V \in \mathcal{C}$  with  $d(V, W) \leq \lfloor (d_S(\mathcal{C}) - 1)/2 \rfloor$ , where  $d_S(\mathcal{C})$  denotes the minimum subspace distance of  $\mathcal{C}$ . Then  $W \otimes_{\mathbb{F}} R$  is decodable in the submodule code  $\mathcal{C} \otimes_{\mathbb{F}} R$ , and it decodes to  $V \otimes_{\mathbb{F}} R$ .

However, there exist submodules of  $R^n$  which are decodable in  $\mathcal{C} \otimes_{\mathbb{F}} R$  but are not of the form  $W \otimes_{\mathbb{F}} R$ , with  $W$  an  $\mathbb{F}$ -space which is decodable in  $\mathcal{C}$ . Moreover, if  $N \subseteq R^n$  is decodable in  $\mathcal{C} \otimes_{\mathbb{F}} R$ , then  $N \cap \mathbb{F}^n$  is not necessarily decodable in  $\mathcal{C}$ .

Let e.g.  $R = \mathbb{Z}_5[i]$ ,  $\mathbb{F} = \mathbb{Z}_5$ , and let  $\mathcal{C} = \{V_1, V_2\} \subseteq \mathcal{M}(\mathbb{Z}_5^4)$  be the subspace code whose codewords are the 2-dimensional spaces

$$V_1 = \langle (1, 0, 1, 0), (0, 1, 0, 1) \rangle_{\mathbb{Z}_5}, \quad V_2 = \langle (1, 0, 2, 1), (0, 1, 1, 0) \rangle_{\mathbb{Z}_5}.$$

Then  $\mathcal{C}$  has subspace distance  $d_S(\mathcal{C}) = 4$ . By Theorem 50 the submodule code  $\mathcal{C} \otimes_{\mathbb{Z}_5} \mathbb{Z}_5[i]$  has two codewords of length 4 and submodule distance  $d(\mathcal{C} \otimes_{\mathbb{Z}_5} \mathbb{Z}_5[i]) = 8$ .

Let

$$N = \langle (i + 2, 0, i + 2, 0), (0, 1, 0, i - 1) \rangle_{\mathbb{Z}_5[i]} \subseteq \mathbb{Z}_5[i]^4$$

be a received submodule. Then  $d(N, V_1 \otimes_{\mathbb{Z}_5} \mathbb{Z}_5[i]) = 3 \leq \lfloor (8 - 1)/2 \rfloor = 3$ , so  $N$  is decodable in  $\mathcal{C} \otimes_{\mathbb{Z}_5} \mathbb{Z}_5[i]$ . However,  $N$  is not of the form  $W \otimes_{\mathbb{Z}_5} \mathbb{Z}_5[i]$  for any vector space  $W$ . Moreover,  $N \cap \mathbb{Z}_5^4 = 0$ , so  $N \cap \mathbb{Z}_5^4$  is not decodable in  $\mathcal{C}$  with respect to the subspace distance.

### 5.3 Two constructions over products of rings

Let  $R \cong R_1 \times \dots \times R_m$ , where  $R_1, \dots, R_m$  are finite commutative rings with identity. Let  $\pi_i$  be the projection on the factor  $R_i$ . Then each  $\pi_i$  extends componentwise to a map  $\pi_i : R^n \rightarrow R_i^n$ .

**Lemma 53.** Let  $R \cong R_1 \times \dots \times R_m$  be a finite ring, let  $M \subseteq R^n$  be an  $R$ -module. Then  $M \cong \pi_1(M) \times \dots \times \pi_m(M)$ , each  $\pi_i(M)$  is an  $R_i$ -module and

$$\lambda_R(M) = \sum_{i=1}^m \lambda_{R_i}(\pi_i(M)).$$

*Proof.* Let  $r_i \in R_i$  and  $v \in M$ . Then  $\pi_i(v) = (\pi_i(v_1), \dots, \pi_i(v_n)) \in \pi_i(M) \subseteq R_i^n$ , and  $r_i \pi_i(v) = (r_i \pi_i(v_1), \dots, r_i \pi_i(v_n)) \in \pi_i(M)$ . This makes  $\pi_i(M)$  into an  $R_i$ -module. Moreover, the isomorphism  $R^n \cong R_1^n \times \dots \times R_m^n$  restricts to an isomorphism  $M \cong \pi_1(M) \times \dots \times \pi_m(M)$ . Hence

$$\lambda_R(M) = \sum_{i=1}^m \lambda_R(\pi_i(M)) = \sum_{i=1}^m \lambda_{R_i}(\pi_i(M)),$$

where the last equality follows from the fact that any  $R$ -submodule of  $\pi_i(M)$  is an  $R_i$ -submodule, and viceversa.  $\square$

We start with a simple construction, where we produce a code over  $R_1 \times \dots \times R_m$  by taking the cartesian product of codes over each  $R_i$ . For simplicity of notation we identify  $R^n$  and  $R_1^n \times \dots \times R_m^n$ .

**Theorem 54.** Let  $R_1, \dots, R_m$  be finite PIR's and let  $R = R_1 \times \dots \times R_m$ . For  $i \in \{1, \dots, m\}$  let  $\mathcal{C}_i \subseteq \mathcal{M}(R_i^n)$  be a submodule code whose codewords have length  $k_i$ . Then

$$\mathcal{C} = \mathcal{C}_1 \times \dots \times \mathcal{C}_m = \{M_1 \times \dots \times M_m : M_i \in \mathcal{C}_i \text{ for all } i\} \subseteq \mathcal{M}(R^n)$$

is a submodule code of cardinality  $|\mathcal{C}| = |\mathcal{C}_1| \dots |\mathcal{C}_m|$ , whose codewords have length  $k_1 + \dots + k_m$ , and with minimum distance  $d(\mathcal{C}) = \min\{d(\mathcal{C}_i) : 1 \leq i \leq m\}$ .

We now show that decoding of the **product code**  $\mathcal{C} = \mathcal{C}_1 \times \dots \times \mathcal{C}_m$  over  $R$  can be reduced to decoding each of the codes  $\mathcal{C}_i$  over  $R_i$ .

**Proposition 55.** Let  $R_1, \dots, R_m$  be finite PIR's and let  $R = R_1 \times \dots \times R_m$ . For  $i \in \{1, \dots, m\}$  let  $\mathcal{C}_i \subseteq \mathcal{M}(R_i^n)$  be a submodule code and let  $\mathcal{C} = \mathcal{C}_1 \times \dots \times \mathcal{C}_m \subseteq \mathcal{M}(R^n)$  be the product code. Let  $N \subseteq R^n$  be a received decodable submodule, i.e., an  $R$ -module for which there exists an  $M = M_1 \times \dots \times M_m \in \mathcal{C}$  such that  $d(N, M) \leq \lfloor (d(\mathcal{C}) - 1)/2 \rfloor$ . Then for all  $i \in \{1, \dots, m\}$  we have  $d(\pi_i(N), M_i) \leq \lfloor (d(\mathcal{C}_i) - 1)/2 \rfloor$ , i.e.,  $\pi_i(N)$  decodes to  $M_i$  in  $\mathcal{C}_i$ .

*Proof.* By Lemma 53,  $N = \pi_1(N) \times \dots \times \pi_m(N)$ , and  $M_i = \pi_i(M)$  for  $1 \leq i \leq m$ . Moreover

$$\begin{aligned} d(N, M) &= \lambda(N) + \lambda(M) - 2\lambda(N \cap M) \\ &= \sum_{i=1}^m \lambda_{R_i}(\pi_i(N)) + \sum_{i=1}^m \lambda_{R_i}(\pi_i(M)) - 2 \sum_{i=1}^m \lambda_{R_i}(\pi_i(N \cap M)) \\ &\geq \sum_{i=1}^m d(\pi_i(N), \pi_i(M)), \end{aligned}$$

where the inequality follows from the fact that  $\pi_i(N \cap M) \subseteq \pi_i(N) \cap \pi_i(M)$ . Therefore for all  $i$  we have

$$d(\pi_i(N), \pi_i(M)) \leq d(N, M) \leq \lfloor (d(\mathcal{C}) - 1)/2 \rfloor \leq \lfloor (d(\mathcal{C}_i) - 1)/2 \rfloor,$$

hence  $\pi_i(N)$  decodes to  $M_i$  in  $\mathcal{C}_i$ .  $\square$

Finally, we provide another construction which combines submodule codes over the factors  $R_i$  into a submodule code over  $R = R_1 \times \dots \times R_m$ . Compared to the product construction of Theorem 54, this construction produces a code with smaller cardinality and larger minimum distance, whose decoding cannot be reduced to decoding over the  $R_i$ 's. Again, for simplicity we identify  $R^n$  and  $R_1^n \times \dots \times R_m^n$ .

**Theorem 56.** Let  $R_1, \dots, R_m$  be finite PIR's, and let  $R = R_1 \times \dots \times R_m$ . For  $i \in \{1, \dots, m\}$  let  $\mathcal{C}_i \subseteq \mathcal{M}(R_i^n)$  be a submodule code whose codewords have length  $k_i$ . Let  $c = \min |\mathcal{C}_i|$ , and for all  $i \in \{1, \dots, m\}$  fix a subcode  $\mathcal{C}'_i \subseteq \mathcal{C}_i$  with  $|\mathcal{C}'_i| = c$ . Enumerate the elements of each  $\mathcal{C}'_i$  as  $\mathcal{C}'_i = \{M_{1,i}, \dots, M_{c,i}\}$ . Then

$$\mathcal{C} = \{M_{j,1} \times \dots \times M_{j,m} : 1 \leq j \leq c\} \subseteq \mathcal{M}(R^n)$$

is a submodule code of cardinality  $|\mathcal{C}| = c$ , with  $d(\mathcal{C}) \geq d(\mathcal{C}_1) + \dots + d(\mathcal{C}_m)$ , and whose codewords have length  $k_1 + \dots + k_m$ .

*Proof.* We only prove the part about the minimum distance. Let  $j, j' \in \{1, \dots, c\}$  with  $j \neq j'$ . Arguing as in the proof of Proposition 55, one finds

$$d(M_{j,1} \times \dots \times M_{j,m}, M_{j',1} \times \dots \times M_{j',m}) \geq \sum_{i=1}^m d(M_{j,i}, M_{j',i}) \geq \sum_{i=1}^m d(\mathcal{C}_i),$$

where the last inequality follows from the fact that  $M_{j,i} \neq M_{j',i}$  whenever  $j \neq j'$ .  $\square$

**Remark 57.** Notice that an  $R$ -module which is decodable with respect to the code  $\mathcal{C}$  constructed in Theorem 56 is not necessarily a product of  $R_i$ -modules that are decodable with respect to the codes  $\mathcal{C}_i$ . E.g., let  $m = 2$ ,  $n = 4$ ,  $R_1 = R_2 = \mathbb{Z}_2$ ,  $R = \mathbb{Z}_2 \times \mathbb{Z}_2$ . Let

$$M_{1,1} = M_{1,2} = \langle (1, 0, 1, 0), (0, 1, 0, 1) \rangle_{\mathbb{Z}_2}, \quad M_{2,1} = M_{2,2} = \langle (1, 0, 1, 1), (0, 1, 1, 0) \rangle_{\mathbb{Z}_2}$$



and  $\mathcal{C}_1 = \mathcal{C}'_1 = \{M_{1,1}, M_{1,2}\}$ ,  $\mathcal{C}_2 = \mathcal{C}'_2 = \{M_{2,1}, M_{2,2}\}$ . Then

$$\mathcal{C} = \left\{ \text{row} \begin{bmatrix} (1,1) & (0,0) & (1,1) & (0,0) \\ (0,0) & (1,1) & (0,0) & (1,1) \end{bmatrix}, \text{row} \begin{bmatrix} (1,1) & (0,0) & (1,1) & (1,1) \\ (0,0) & (1,1) & (1,1) & (0,0) \end{bmatrix} \right\}.$$

The code  $\mathcal{C}$  has minimum distance  $d(\mathcal{C}) = 8$ . Let

$$N = \text{row} \begin{bmatrix} (1,0) & (0,0) & (1,0) & (0,0) \\ (0,0) & (1,1) & (0,1) & (1,1) \end{bmatrix}$$

be a received submodule. Then  $N$  decodes to  $M_{1,1} \times M_{1,2} \in \mathcal{C}$ , as  $d(N, M_{1,1} \times M_{1,2}) = 3 \leq \lfloor (8-1)/2 \rfloor$ . However,  $\pi_2(N) = \langle (0, 1, 1, 1) \rangle_{\mathbb{Z}_2}$  is not decodable in  $\mathcal{C}_2$ . In fact,  $d(\pi_2(N), M_2^1) = d(\pi_2(N), M_2^2) = 3$ .

## References

- [1] D. D. Anderson, M. Axtell, S. J. Forman, J. Stickles, *When are Associates Unit Multiples?*, Rocky Mountain Journal of Mathematics 34 (2004), no. 3, 811–828.
- [2] J. Buchmann, S. Neis, *Algorithms for linear algebra problems over principal ideal rings*, technical report, Technische Hochschule Darmstadt (1996).
- [3] P. Delsarte, *Bilinear forms over a finite field, with applications to coding theory*, Journal of Combinatorial Theory, Series A, 25 (1978), no. 3, 226 – 241.
- [4] C. Feng, R. W. Nóbrega, F. R. Kschischang, D. Silva, *Communication over finite-chain-ring matrix channels*, IEEE Transactions on Information Theory 60 (2014), no. 10, 5899–5917.
- [5] C. Feng, D. Silva, F. R. Kschischang, *An algebraic approach to physical-layer network coding*, IEEE Transactions on Information Theory 59 (2013), no. 11, 7576–7596.
- [6] E. Gorla, A. Ravagnani, *Partial spreads in random network coding*, Finite Fields and Their Applications 26 (2014), 104–115.
- [7] J. A. Howell, *Spans in the module  $(\mathbb{Z}_m)^s$* , Linear and Multilinear Algebra 19 (1986), 67–77.
- [8] R. Kötter, F. R. Kschischang, *Coding for errors and erasures in random network coding*, IEEE Transactions on Information Theory 54 (2008), no. 8, 3579–3591.
- [9] E. Kunz, *Introduction to commutative algebra and algebraic geometry*, Birkhäuser Boston Inc., Boston (1985).
- [10] B. R. McDonald, *Finite rings with identity*, Pure and Applied Mathematics 28, Marcel Dekker Inc., New York (1974).
- [11] B. Nazer, M. Gastpar, *Compute-and-forward: harnessing interference through structured codes*, IEEE Transactions on Information Theory 57 (2011), no. 10, 6463–6486.
- [12] P. Popovski, H. Yomo, *The anti-packets can increase the achievable throughput of a wireless multi-hop network*, Proceedings of the IEEE International Conference on Communications 2006, ICC '06, 3885 – 3890.
- [13] Q T. Sun, J. Yuan, T. Huang, K. W. Shum, *Lattice network codes based on Eisenstein integers*, IEEE Transactions on Information Theory 61 (2013), no. 7, 2713–2725.

- [14] O. Zariski, P. Samuel, *Commutative Algebra Vol. 1*, Graduate Texts in Mathematics 28, Springer-Verlag, New York-Heidelberg-Berlin, (1975).
- [15] S. Zhang, S.-C. Liew, P. P. Lam, *Hot topic: physical layer network coding*, Proceedings of the 12th annual international conference on Mobile computing and networking, MobiCom '06, 358–365.